The Auditor-General
Audit Report No.25 2009–10
Performance Audit

Security Awareness and Training

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 81115 6

Australian National
Audit Office

Canberra ACT
15 April 2010

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*. Pursuant to *Senate Standing Order 166* relating to the presentation of documents when the Senate is not sitting, I present the report of this audit and the accompanying brochure. The report is titled *Security Awareness and Training.*

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

Yours sincerely

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 (ANAO). 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 Australian 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
Rowena Hayman
Caroline Smith
Bill Bonney
Stuart Turnbull

Contents

Tables

Figures

Abbreviations

AGD	Attorney-General's Department
ALRC	Australian Law Reform Commission
ANAO	Australian National Audit Office
APS	Australian Public Service
Archives	National Archives of Australia
ASA	Agency Security Adviser
CAC Act	*Commonwealth Authorities and Companies Act 1997*
CrimTrac	CrimTrac Agency
DSD	Defence Signals Directorate
Gallery	National Gallery of Australia
Health	Department of Health and Ageing
ICT	Information Communications and Technology
ISM	Information Security Manual
ITSA	Information Technology Security Adviser
PSM	Protective Security Manual

Glossary

Agency Security Adviser	The person responsible for the day-to-day performance of the protective security functions within an organisation.
Information security	The policies and practices used in the protection of hard copy and electronic information (such as records, documents, papers and data), as well as the systems on which information is stored, processed or communicated.
Information communications and technology (ICT) security	A subset of information security, which is specifically concerned with the protection of electronic information and systems.
Information system security accreditation	The process by which an authoritative body accepts and gives approval that the residual risks relating to the operation of an information system are appropriate. The security accreditation process involves assessing whether there are sufficient security measures, policies and procedures in place to protect the information that is processed, stored or communicated by that system.
Information Technology Security Adviser	The person responsible for information communications and technology related security functions within an organisation.
Personnel security	Policies and procedures designed to assess, on an ongoing basis, the eligibility and suitability of individuals requiring access to security classified information and resources.
Physical Security	Policies and procedures designed to prevent unauthorised access to official resources and to detect and respond to intrusions, as well as maintain a safe and secure environment for the protection of the organisation's employees and clients.

Protective security	The collective term for the range of policies and practices employed to assist in the protection of an organisation's resources. Typically, protective security arrangements encompass policies and practices across information, ICT, personnel and physical security dimensions.
Security awareness	Understanding and appreciating the security risks and threats faced by an organisation, the responsibilities associated with the security policies and practices put in place to address those risks, and the costs of losing or compromising official resources.
Security classified resources	Resources that require additional layers of protection because they are critical to the performance of government functions; or because their loss, compromise or misuse could harm Australia's national security or adversely impact on the interests of the community.
Security clearance	An administrative determination that an individual is eligible and suitable, from a security standpoint, for access to security classified resources.
Security Executive	A member of an organisation's senior management group (typically a member of the Senior Executive Service) who has overall responsibility for protective security functions in the organisation.
Security risk	An event that could result in the compromise of official resources, measured in terms of its likelihood and consequences.

Summary and Recommendations

Summary

Introduction

1. Australian Government organisations have access to, and manage a significant amount of official resources, including information and assets. All individuals working in these organisations have a responsibility to protect and properly use these resources.

2. The policies and practices used to assist in the protection of these resources are collectively known as 'protective security'. Protective security arrangements typically encompass information, information communications and technology (ICT), personnel and physical security dimensions.

3. A program of security awareness and training activities, which reflects an organisation's circumstances and risks, is integral to having effective protective security arrangements more broadly. Specifically, organisations need measures to help ensure that individuals who have access to official resources are aware, and as appropriate, trained in the application of any relevant security policies and procedures. This includes providing them with a clear understanding of their security related responsibilities.

4. The *Protective Security Manual* (PSM) and the *Information Security Manual* (ISM) contain the Australian Government's policy, guidelines and minimum requirements relating to the protection of official resources.[1] Both manuals outline the importance of, and contain requirements relating to, the provision of security awareness and training.

5. In addition to the requirements in the PSM and ISM, there is a wide range of legislative obligations relating to the protection, use and disclosure of information. The Australian Law Reform Commission (ALRC) recently reported that it had identified 506 'secrecy' provisions among 176 different pieces of primary and subordinate Commonwealth legislation.[2] Some of these provisions are organisation-specific, contained in legislation administered by

---

[1] Attorney-General's Department, *Protective Security Manual,* October 2007 and Defence Signals Directorate, *Information Security Manual*, September 2009. The scope of each manual is discussed in Chapter 1.

[2] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 70. The 506 provisions are listed in Appendix 4 of the Report (pp. 613-629). The report is available at: <www.alrc.gov.au/inquiries/title/alrc112/index.html> [accessed 12 March 2010].

the organisation, or in some cases, in its enabling legislation. In other instances, the provisions have broad application among Australian Government organisations, such as those in the *Public Service Act 1999*.

6. An organisation's security awareness and training program should promote an understanding of those requirements in the PSM and ISM that are pertinent to the roles and responsibilities of its staff. In this regard, requirements that are likely to have general application to the majority of Australian Government organisations include:

- handling, storing and disposing of official information, including security classified information;
- determining the security classification of information, including the use of protective markings;
- responsibilities associated with holding a security clearance, including reporting any changes in circumstances; and
- maintaining sound physical security polices and procedures, including perimeter and work area access controls, the wearing of staff passes and the management of keys and combinations.

7. The PSM recognises that other legislation contains requirements relating to the protection of particular types of official information. Accordingly, it is good practice for an organisation's security awareness program to also promote an understanding of any relevant 'confidentiality' obligations in legislation administered by, or affecting the organisation.

8. More broadly, security awareness and training activities are likely to be more effective if organisational-wide security risks and issues are assessed, and the results used to plan security awareness and training activities. The impact of security awareness messages will be more beneficial if they are promoted and regularly reinforced using a variety of methods. In addition, the design of security awareness activities should take into account such things as: the nature of the organisation's information holdings and physical assets; the number of operational sites; and the number of staff with security clearances.

9. Since 1995, the Australian National Audit Office (ANAO) has undertaken ten cross-agency audits of protective security arrangements in Australian Government organisations.[3] As shown in Table S 1, three of these

[3] These audits are listed at Appendix 2.

audits have included recommendations designed to improve the management and delivery of security awareness and training. Each of these reports has encouraged Australian Government organisations to assess the benefits of the recommendations in light of their own circumstances and practices.

Table S 1

Recommendations relating to security awareness and training in previous ANAO protective security audit reports

Reference	Description
Audit Report No.23 2002–03 *Physical Security Arrangements in Commonwealth Agencies*	The ANAO **recommends** that agencies develop and schedule periodic education and awareness programs for non-security personnel addressing agency security standards (Recommendation No.3).
Audit Report No.55 2003–04 *Management of Protective Security*	The ANAO **recommends** that organisations develop and implement a structured and proactive security awareness education and training strategy (Recommendation No.2).
Audit Report No.41 2007–08 *Management of Personnel Security Follow-up Audit*	The ANAO **recommends** that organisations promote security aftercare arrangements in security education and training activities (Recommendation No.2).

Source: ANAO.

Audit approach

10. The objective of the audit was to assess the effectiveness of security awareness and training arrangements at selected Australian Government organisations, including whether they addressed selected security issues from the PSM.

11. To address the audit objective, the ANAO examined the methods used to promote and deliver security awareness and training, and whether the success (or otherwise) of these activities was being actively measured. The audit also assessed whether the three relevant recommendations from the ANAO's previous protective security audits have been implemented.

12. The audit also obtained details of progress made by the Attorney-General's Department and the Department of Finance and Deregulation in clarifying which organisations operating under the *Commonwealth Authorities and Companies Act 1997* the PSM applies to (Recommendation 1 in ANAO Audit Report No.44 2008–09 *Security Risk Management*).

13. The security awareness and training activities at the following four Australian Government organisations were assessed:

- National Archives of Australia (Archives);
- CrimTrac Agency (CrimTrac);
- National Gallery of Australia (Gallery); and
- Department of Health and Ageing (Health).

14. These organisations face a range of security risks that can affect the integrity of their information and physical resources, their ability to maintain a safe and secure working environment, and the uninterrupted delivery of their programs or services. Specifically:

- central security considerations for the Archives and the Gallery are the protection of high-value and sensitive assets, records and other related information;
- CrimTrac's primary security responsibility is safeguarding the integrity of a range of sensitive law enforcement data, including personal and police reference information; and
- a key security issue for Health is the protection of the wide-range of information that it has access to and administers across its distributed physical locations.

Audit conclusion

15. Protective security describes the range of policies and practices employed to assist in the protection of an organisation's official resources. Soundly designed and timely security awareness and training activities are integral to the maintenance of effective protective security arrangements. Shortcomings in security awareness and training can undermine the operation of the controls and practices put in place to manage exposures to security risks.

16. Overall, the audit concluded that the security awareness and training arrangements at the audited organisations were generally adequate and operating as intended. Nevertheless, there is considerable scope to enhance the effectiveness of the organisations' security awareness and training programs. The main areas for improvement relate to more thoughtful planning, including tailoring the approaches used in light of the organisations' security risk profiles, and better monitoring to help identify security awareness techniques that are not effective or working well. In addition, the audited organisations

would benefit from improved record keeping to assist them manage the timely delivery of, and attendance at, security awareness training.

17. The audited organisations use a variety of approaches to promote and reinforce security awareness, including providing information on security requirements as part of staff induction processes, and offering ongoing security training or briefings to all staff. For the most part, the content of each organisation's[4] security awareness and training programs adequately reflects the organisation's circumstances, including its security risks and issues[5], and provides good coverage of selected security issues from the PSM. On the other hand, only two of the audited organisations adequately cover the confidentiality and protection of information requirements contained in the *Public Service Act 1999*.

18. Procedures are in place to identify and capture details of security breaches or incidents at each of the audited organisations. At two of the audited organisations, less than five per cent of the security incidents examined were indicative of security awareness issues. However, around 40 per cent of the security incidents examined at another organisation related to a similar issue, suggesting a potential shortcoming in security awareness levels.

19. The principal shortcomings identified during the audit are:

- three of the organisations did not have a sound, organisation-wide approach to identifying and assessing security risks and, as a result, could not demonstrate that the security risks faced by the organisation were appropriately factored into the design of their security awareness and training programs;
- only one organisation had an approved security awareness and training plan setting out its approach to managing its security awareness program;
- none of the organisations had training targeted at the roles and responsibilities of security cleared staff, although one organisation provides guidance (annually) to these staff about their responsibilities;

[4] Except CrimTrac, as the ANAO did not assess the content of its security awareness and training program (see paragraph 44).

[5] Based on the five elements examined by the ANAO (see paragraph 39).

- records on the delivery of, and attendance at security awareness training were limited and, where available, generally indicated a need for additional, and more timely training; and
- none of the organisations regularly monitored the effectiveness of their security awareness and training programs, although two organisations monitored security incident records to help inform the design of their security awareness and training activities.

20. Three of the key findings in this audit (the lack of structured and organisation-wide security risk assessments, the lack of security awareness planning; and the lack of monitoring) are consistent with findings reported in previous ANAO protective security audits. This suggests that improvements in these areas remain elusive for Australian Government organisations.

21. Health had implemented each of the three relevant recommendations from previous ANAO protective security audits. Archives had implemented two, the Gallery had implemented one and partially implemented another of the recommendations, while CrimTrac had partially implemented two of the recommendations.

22. The audit makes one recommendation aimed at improving organisations' approaches to security risk management. The remaining four recommendations of the audit are designed to improve the management of security awareness and training activities. Specifically, these recommendations focus on enhancing the planning, design, record keeping and monitoring of such activities. One of these recommendations (Recommendation No.2) reiterates similar recommendations made in previous ANAO audit reports.

Key findings by Chapter

Supporting Security Awareness and Training (Chapter 2)

Assessing security risks

23. Organisations should adopt a structured and organisation-wide approach to identify, assess, treat, and monitor their protective security risks. Such an approach increases the likelihood that relevant security risks and issues will be appropriately factored into the organisation's security awareness and training activities.

24. The Gallery was the only organisation that had undertaken an organisation-wide review to identify and assess its security risks, including the

risks associated with security awareness and training. The effectiveness of the approaches adopted at the other organisations was limited because:

- not all aspects of security risks were addressed – for example, Archives had not assessed risks associated with its security awareness and training activities and CrimTrac did not have up-to-date security risk assessments for its key ICT systems;
- no consolidated records of security risks were maintained, including their assessment, associated mitigation measures and the assignment of responsibilities for managing the security risks; and
- the results of security risk activity were not endorsed by the organisations' senior management.

25. The results of the audit indicate there is scope to improve the approaches of the audited organisations to identify and assess their security risks. ANAO Recommendation No.1 is designed to address these issues.

Security policies have been promulgated and are current

26. Clear, current and easily accessible security policies, together with related procedural documentation, are important to assist staff better understand an organisation's security risks and issues, as well as their own security related responsibilities.

27. Each of the audited organisations had a range of readily accessible security policy and procedural documents. The documents were generally comprehensive, dealing with relevant security issues and requirements in an informative manner. Importantly, the security policy documents at the Gallery and Health had been recently reviewed and endorsed by their respective senior management. The Archives and CrimTrac would benefit from a review of the currency of their documents, including an assessment of whether they remain consistent with relevant standards in the PSM and the ISM.

Communication with senior management

28. Strong direction, leadership and commitment from an organisation's senior management are important in achieving effective protective security outcomes. As noted in Audit Report No.44 2008–09, *Security Risk Management*, organisations should have regular communication lines to support senior managers to obtain sufficient understanding and assurance about security related matters.

29. Each of the audited organisations had designated a member of their senior management to oversee the management of protective security matters within the organisation (commonly known as the Security Executive). In each case, this person maintained regular contact with the organisation's security team.

30. CrimTrac, the Gallery and Health regularly reported on security related matters to their respective senior management. There would be merit in the Archives reporting periodically on the status or performance of protective security activities to senior management.

Security awareness and training planning

31. Planning can assist an organisation develop coordinated and targeted security awareness and training programs, and help ensure that activities are designed to suit the roles and responsibilities of staff. The form and extent of planning required by each organisation depends on the organisation's circumstances, including its size, the nature of operations and its security risk profile.

32. Health, which was the largest organisation audited, was the only organisation that had an approved security awareness and training plan in place. Health's plan contains a series of strategies designed to improve the department's approach to security awareness and training. The strategies include undertaking targeted audience assessments, using available communication channels effectively, and monitoring and evaluation arrangements.

33. The lack of planning of security awareness and training activities is consistent with the results in previous ANAO protective security audits. ANAO Recommendation No.2 is designed to address this issue.

Designing and Delivering Security Awareness and Training (Chapter 3)

Security awareness techniques

34. Security awareness messages will be more effective when promoted and reinforced on a regular basis using a variety of mechanisms or tools. This normally requires a mix of general (organisation-wide) and targeted (role or work area specific) mechanisms; and the use of both active (such as briefings) and passive (such as posters) methods.

35. For the most part, the audited organisations employed a good variety of security awareness techniques. Specifically, each of the audited organisations provided security awareness training as part of their induction process, as well as offering ongoing security awareness training or briefings. However, only the Gallery and Health used posters or brochures to promote key security related messages.

36. The Gallery and Health had both recently introduced e-learning applications that contain modules dealing with security, including ICT security. Other useful techniques used by the audited organisations included a requirement for staff to sign security related acknowledgements or declarations and the promulgation of a series of factsheets on selected security issues.

Sufficiency and appropriateness of the content of security awareness and training programs

37. The design of an organisation's security awareness and training program should be commensurate with the nature of the organisation's operations, including its security risks and issues.

38. As mentioned at paragraph 24, the Gallery was the only organisation that had undertaken an organisation-wide review to identify and assess its security risks and that maintained sufficient documentation of its security risks. As result, the organisations could not clearly demonstrate that details of security risks were appropriately factored into the design of their security awareness and training programs.

39. Consequently, the ANAO examined whether the content (and design) of the audited organisations' security awareness and training programs reflected the:

- nature of the organisation's information holdings, including the level of security classified and sensitive information;
- number of staff with security clearances;
- location, nature and value of physical assets;
- number of the organisation's operational sites; and
- existence of any specific requirements relating to the protection and confidentiality of information in legislation or agreements administered by the organisation.

40. Overall, the ANAO assessed that the content of the security awareness and training programs at the Archives, the Gallery and Health was, for the most part, sufficient and appropriate in terms of the elements examined. Specifically, the design of the security awareness and training material at each organisation adequately reflected the nature of that organisation's information holdings, the value of its physical assets and the number (and location) of operational sites. In addition, the programs at each organisation largely addressed the selected issues from the PSM that were examined by the ANAO.

41. The security awareness material at the Gallery and Health adequately covered the requirements for the protection of information contained in the *Public Service Act 1999.* New starters at the Archives are required to acknowledge that they have been made aware of these requirements. However, two-thirds of Archives' personnel files examined by the ANAO did not contain documentation to indicate the acknowledgement had occurred.

42. The audit identified a number of opportunities to further improve the design of the organisations' security awareness training activities, including:

- none of the organisations had any training or briefings targeted at the roles and responsibilities of security cleared staff, although the Gallery reminds security cleared staff of their responsibilities through an annual acknowledgement form;
- not all of the security awareness training material at the Archives and the Gallery contained references to the availability of their respective security policy and procedural documents; and
- the security awareness training material at the Archives did not contain information on, or references to, requirements contained in the *Archives Act 1983* relating to the protection of information.

43. ANAO Recommendation No.3 is aimed at addressing these findings.

44. At the time of the audit CrimTrac's security policy document was more than five years old. CrimTrac advised that it plans to review this document, and update it as necessary. The ANAO did not assess the content of CrimTrac's security policy document as it intends to replace it. CrimTrac discontinued use of the Attorney-General's Department's Internet-based security awareness training program in March 2009, and during the audit was re-assessing its approach to security awareness training. As a result, CrimTrac did not have a structured security awareness training program in place at the

time of the audit. The ANAO did not assess the content of the training material as it is no longer being used by CrimTrac.

Maintaining sufficient records on the delivery of security awareness training

45. Maintaining accurate and complete attendance information can help organisations manage the scheduling and delivery of security awareness training. Accurate attendance records also provide assurance to senior management that sufficient training has occurred.

46. Apart from the Gallery, none of the audited organisations maintained sufficient records on the delivery of, and attendance at, security awareness training. The introduction of e-learning applications at two of the organisations has resulted in the capture of more accurate and detailed information on the completion of security awareness training. The lack of structured records meant there was insufficient evidence to gain assurance that appropriate levels of security awareness training had occurred. However, the records that were available suggest that the audited organisations can improve both the amount and the timeliness of security awareness training. ANAO Recommendation No.4 is designed to address these issues.

Monitoring the Effectiveness of Security Awareness and Training (Chapter 4)

47. Organisations that regularly monitor and assess the effectiveness of security awareness and training activities are well placed to make timely improvements to the approaches they use. This includes detecting delivery techniques that are not working well, or are no longer useful.

48. None of the audited organisations had regular and structured processes in place to assess the impact and success (or otherwise) of their security awareness and training activities. ANAO Recommendation No.5 is aimed at addressing this finding.

49. The organisations did, however, use a range of intermittent processes to obtain information on security awareness levels. For example, the Gallery and Health periodically monitored security incident records. Security incidents can provide valuable insights into an organisation's security environment, including the level of security awareness. Each of the audited organisations had implemented procedures to identify and capture details of security breaches or incidents. An examination of security incidents records at three of the audited organisations (at the time of the audit, no security incidents were

recorded at CrimTrac) indicated that incidents were well documented, with follow-up action generally occurring in a timely manner.

Summary of organisations' responses

50. Each of the audited organisations, together with AGD, agreed with the recommendations in the report. The organisations' responses to each recommendation are included under the sub-heading 'Organisations' responses' directly following each recommendation. General comments on the proposed audit report provided by the audited organisations, together with comments from AGD and Finance, are contained in Appendix 1.

Recommendations

The recommendations are based on findings from fieldwork at the audited 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 2.12

The ANAO recommends that organisations assess their approach to the identification, analysis and monitoring of security risks against the guidance contained in Part B of the *Protective Security Manual*.

Recommendation No.2

Para 2.40

The ANAO recommends that Australian Government organisations develop a security awareness and training plan that is commensurate with the organisation's circumstances, including its size and security risk profile, and that reflects the relevant requirements in the *Protective Security Manual* and the *Information Security Manual*.

Recommendation No.3

Para 3.40

The ANAO recommends that organisations' security awareness training programs are tailored to reflect the organisation's security risks and issues. This includes, as appropriate, having training on:

- the responsibilities of security cleared staff;
- the organisation's key security policies and procedures; and
- any requirements relating to the protection of information in legislation or agreements administered by, or affecting, the organisation.

Recommendation No.4

Para 3.53

To assist in the provision of appropriate and timely training, the ANAO recommends that organisations maintain accurate and complete records of the delivery of, and attendees at, security awareness training.

Recommendation No.5

Para 4.17

The ANAO recommends that organisations implement cost-effective arrangements to periodically monitor the effectiveness of their security awareness and training activities.

Audit Findings and Conclusions

1. Introduction

This chapter provides background information about the audit, including an overview of the Australian Government's protective security requirements, and details of relevant previous audit coverage.

Protective security

1.1 Australian Government organisations have access to, and manage a significant amount of official resources, including information and assets. All individuals working in these organisations have a responsibility to protect and properly use these resources. Additional layers of protection are required for those resources that have been assessed as being critical to the performance of government functions; or because their loss, compromise or misuse could harm Australia's national security or adversely impact on the interests of the community.[6]

1.2 The policies and practices used to assist in the protection of official resources are collectively known as 'protective security'. Protective security arrangements typically encompass the following dimensions:

- information security—includes the handling, storage and classification of official information;
- information communications and technology (ICT) security—includes logical access controls, the protection of software, data storage and transmission and network connectivity issues;
- personnel security—includes the processing of security clearances for staff with access to classified information or resources; and
- physical security—includes the operation of perimeter and building access controls and alarm systems.

1.3 A program of security awareness and training activities, which reflects an organisation's circumstances and risks, is integral to effective protective security arrangements more broadly. Specifically, organisations need measures to help ensure that individuals with access to official resources are aware, and

[6] The *Protective Security Manual* requires such resources to be security classified. Refer to Part C of the manual.

as appropriate, trained in the application of any relevant security policies and procedures. This includes providing them with a clear understanding of their security related responsibilities.

1.4 A security awareness program should be designed to:

- promote the need for security and provide individuals with an understanding of their security responsibilities;
- maximise the contribution of individuals to the organisation's protective security practices, including by increasing adherence to security policies and controls; and
- explain the potential implications of breaches of security, including the costs of the compromise or loss of assets and information.

The Protective Security Manual and the Information Security Manual

1.5 The *Protective Security Manual* (PSM) and the *Information Security Manual* (ISM) contain the Australian Government's policy, guidelines and minimum requirements relating to the protection of official resources.[7] Both manuals outline the importance of, and contain requirements relating to, the provision of security awareness and training.

1.6 The PSM contains guidance and requirements across each of the dimensions of protective security (information, ICT, personnel and physical). The PSM includes only relatively high-level advice about ICT security, and states that organisations must comply with the requirements of the ISM.[8] The ISM contains detailed guidance and requirements relating to the protection of information that is processed, stored and communicated by ICT systems.[9]

---

[7] Attorney-General's Department, *Protective Security Manual,* October 2007 and Defence Signals Directorate, *Information Security Manual*, September 2009.

[8] Prior to its release in September 2009, the ISM was called the *Information and Communications Technology Security Manual* (known as ACSI 33). The ISM was released following a major review of ICT security policy and requirements.

[9] Chapter 3 lists the requirements in these manuals that are likely to have general application to the majority of Australian Government organisations.

Applicability of the PSM

1.7 The Australian National Audit Office's (ANAO's) Audit Report No.44 2008–09, *Security Risk Management* highlighted uncertainty regarding the applicability of the PSM to organisations operating under the *Commonwealth Authorities and Companies Act 1997* (CAC Act).

1.8 This uncertainty stemmed from a lack of visibility as to which CAC Act organisations have received a direction, from their responsible Minister, under (the former) sections 28 or 43 of the Act to apply the PSM.[10] Concomitantly, there was a risk that some CAC Act organisations may not be aware of legal advice from the Australian Government Solicitor (AGS) that indicates that CAC Act organisations with employees engaged under the *Public Service Act 1999* may be obliged to comply with the PSM even when they have not been directed to do so. As a result, the ANAO recommended that the Attorney-General's Department (AGD) work with the Department of Finance and Deregulation (Finance) to clarify to which CAC Act organisations the PSM applies.[11]

1.9 AGD and Finance have advised that they have commenced work to clarify the application of the PSM to CAC Act organisations. Key elements of the work to date are:

- Finance obtained advice from the AGS clarifying that the requirements of the *Public Service Act 1999* cannot be relied upon as a basis for applying the PSM to CAC Act organisations simply by virtue of the fact that (some) employees are subject to that Act;[12]
- AGD advised that it is currently reviewing the Australian Government's protective security requirements, and anticipates releasing a new protective security policy framework in mid-2010.

[10] Amendments to the CAC Act (which came into effect on 1 July 2008) changed the way in which the 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 their responsible Minister.

[11] ANAO, Audit Report No.44 2008–09, *Security Risk Management*, p. 32. Available at: <http://www.anao.gov.au/director/publications/auditreports.cfm>

[12] AGD advised that this legal advice was communicated to protective security practitioners in Australian Government organisations through the *Protective Security Policy* secure website.

AGD advised that the new framework will be designed, among other things, to clarify the applicability of the PSM; and

- Finance advised (and AGD agreed) that a General Policy Order should be issued to formally apply the requirements of the PSM to CAC Act organisations. However, the process to do so, including consultation with affected organisations, will not commence until AGD has completed its review of protective security policy.

Legislative obligations to protect information

1.10 In addition to the requirements in the PSM and ISM, there is a wide range of legislative obligations relating to the protection, use and disclosure of information. The Australian Law Reform Commission (ALRC) recently reported that it had identified 506 'secrecy' provisions among 176 different pieces of primary and subordinate Commonwealth legislation.[13] Some of these provisions are organisation-specific, contained in legislation administered by the organisation, or in some cases, in its enabling legislation. In other instances, the provisions have broad application among Australian Government organisations, such as in the *Public Service Act 1999*, the *Crimes Act 1914* and the *Privacy Act 1988*. The categories of information covered by the 'secrecy' provisions identified by the ALRC include:

- personal information - approximately 30 per cent of the secrecy provisions identified by the ALRC prohibit the disclosure of personal information;
- confidential information, including the disclosure of information that was supplied 'in confidence';
- information relating to an investigation, including information about law enforcement operations; and
- any information obtained by a person during the course of their employment.[14]

[13] ALRC, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 70. The 506 provisions identified by the ALRC are listed in Appendix 4 of the Report (pp. 613-629). The report is available at <www.alrc.gov.au/inquiries/title/alrc112/index.html> [accessed 12 March 2010].

[14] ALRC, ibid., pp. 71-77.

1.11 The ALRC's report also identifies the importance of Australian Government organisations developing 'effective information-handling cultures'. In particular, the report states that training and development programs are a key strategy in promoting information-handling obligations among employees, fostering legislative compliance and imparting broader information-handling values.[15] Specifically, the report recommends that:

> Australian Government agencies develop and administer training and development programs for their employees, on induction and at regular intervals thereafter, about the information–handling obligations relevant to their position, including the need to share information in certain situations.

Previous audit coverage of security awareness and training

1.12 This audit is part of a program of cross-agency performance audits that examine processes supporting the delivery of services by Australian Government organisations. These audits are undertaken 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.

1.13 Since 1995, the ANAO has undertaken ten cross-agency audits of the Australian Government's protective security arrangements.[16] As shown in Table 1.1, three of these audits have included recommendations designed to improve the management and delivery of security awareness and training. Each of these reports has encouraged Australian Government organisations to assess the benefits of the recommendations in light of their own circumstances and practices.

[15] ALRC, ibid., pp. 523-530.

[16] These audits are listed at Appendix 2.

Table 1.1

Recommendations relating to security awareness and training in previous ANAO protective security audit reports

Reference	Description
Audit Report No.23 2002–03 *Physical Security Arrangements in Commonwealth Agencies*	The ANAO **recommends** that agencies develop and schedule periodic education and awareness programs for non-security personnel addressing agency security standards (Recommendation No.3).
Audit Report No.55 2003–04 *Management of Protective Security*	The ANAO **recommends** that organisations develop and implement a structured and proactive security awareness education and training strategy (Recommendation No.2).
Audit Report No.41 2007–08 *Management of Personnel Security Follow-up Audit*	The ANAO **recommends** that organisations promote security aftercare arrangements in security education and training activities (Recommendation No.2).

Source: ANAO.

About the audit

Audit objective

1.14 The objective of the audit was to assess the effectiveness of security awareness and training arrangements at selected Australian Government organisations, including whether they addressed selected security issues from the PSM.

1.15 To address the audit objective, the ANAO examined the methods used to promote and deliver security awareness and training, and whether the success (or otherwise) of these activities was being actively measured. The audit also assessed whether the three relevant recommendations from the ANAO's previous protective security audits have been implemented.

Audit scope

1.16 The audit examined security awareness and training activities relating to each of the dimensions of protective security (information, ICT, personnel and physical). Table 1.2 shows the audit themes and criteria used to assess the audited organisations' performance.

Table 1.2

Audit criteria

Audit themes and criteria
Supporting security awareness and training (Chapter 2)
The organisations regularly identify and assess their protective security risks, including the risks associated with security awareness and training activities.
The organisations have promulgated up-to-date protective security policy and procedural documentation, which includes information on security awareness and training activities.
The organisations regularly communicate security information, including security awareness issues, to senior management.
The organisations have approved security awareness and training strategies or plans.
Designing and delivering security awareness and training (Chapter 3)
The organisations use a variety of techniques or approaches to promote security awareness.
The content of security awareness and training programs is sufficient and appropriate in light of: • the organisation's operations, including its security risks and issues; • selected issues from the PSM; and • any relevant legislative requirements relating to protection and confidentiality of information.
Sufficient records are maintained to substantiate the delivery of security awareness and training.
Monitoring the effectiveness of security awareness and training (Chapter 4)
The effectiveness of security awareness and training programs is regularly monitored, including by analysing the impact of security incidents.

Source: ANAO.

Audit approach

1.17 The security awareness and training activities at the following four Australian Government organisations were assessed:

- National Archives of Australia (Archives);
- CrimTrac Agency (CrimTrac);
- National Gallery of Australia (Gallery); and
- Department of Health and Ageing (Health).

1.18 The audit involved interviews with key staff and the examination of protective security plans, policies and guidance, as well as security awareness and training material. The ANAO also reviewed management reports dealing with protective security matters, including the performance of security awareness and training activities. In addition, security awareness training

records and documentation, as well as records of reported security incidents, were examined.

1.19 The audit was conducted in accordance with the ANAO's Auditing Standards at a cost of approximately $225 000.

Security risk profile of the audited organisations

1.20 The audited organisations face a range of security risks that can affect the integrity of their information and physical resources, their ability to maintain a safe and secure working environment, and the uninterrupted delivery of their programs or services. Specifically:

- central security considerations for the Archives and the Gallery are the protection of significant and sensitive assets, records and other related information;
- CrimTrac's primary security responsibility is safeguarding the integrity of a range of sensitive law enforcement data, including personal and police reference information; and
- a key security issue for Health is the protection of the wide range of information that it has access to and administers across its distributed physical locations.

Structure of the audit report

1.21 As well as this introductory chapter, there are three other chapters in this report, which examine whether the audited organisations have:

- appropriate levels of support for security awareness and training (Chapter 2);
- effectively designed and delivered security awareness and training (Chapter 3); and
- processes for monitoring the effectiveness of security awareness and training arrangements (Chapter 4).

2. Supporting Security Awareness and Training

This chapter examines the protective security framework of the audited organisations, and assesses whether there is effective support for security awareness and training.

Introduction

2.1 Thoughtful planning and effective controls will improve the ability of organisations to design, deliver and maintain effective security awareness and training programs. In particular, such arrangements will assist an organisation to better align its security awareness and training activities with the nature of its business, as well as its security risks and issues.

2.2 In this part of the audit, the ANAO examined the processes important to support the design and delivery of security awareness and training activities. Specifically, we examined whether the four audited organisations:

- regularly identify and assess their security risks, including the risks associated with security awareness and training activities;
- have promulgated up-to-date protective security policy and procedural documentation, including information on security awareness and training activities;
- regularly communicate security issues, including information about security awareness and training activities, to senior management; and
- have developed security awareness and training plans.

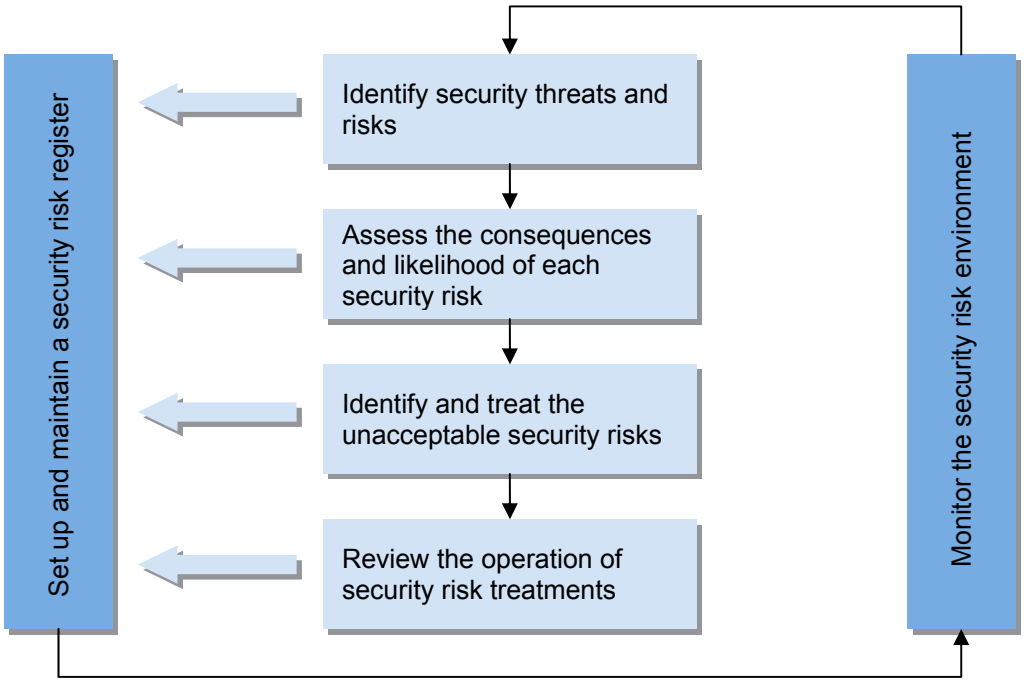
2.3 In examining whether the audited organisations have developed security awareness and training plans, we also assessed the extent that Recommendation No.2 from ANAO Audit Report No.55 2003–04, *Management of Protective Security* has been implemented.

Assessing security risks

2.4 Organisations should adopt a structured and organisation-wide approach to identify, assess, treat, and monitor their security risks[17] and then use the results to help plan their security awareness and training activities. Such a complete approach increases the likelihood that relevant security risks and issues will be appropriately factored into the organisation's security awareness and training activities. Figure 1 illustrates the key components of the structured security risk management process recommended in Part B of the PSM.

Figure 1

Security risk management process



Source: ANAO, based on Part B of the PSM.

2.5 The audited organisations use a variety of approaches to identify and manage their security risks. Overall, the effectiveness of the approaches adopted is limited because they did not always:

[17] ANAO, op. cit., pp. 38-39. This audit has drawn on the results of that audit, especially the findings around the identification and analysis of security risks, but did not seek to duplicate the work undertaken in that audit.

- address all aspects of the organisation's security risks;
- maintain a consolidated record of security risks, including their assessment and the associated treatment or mitigation measures;
- have a clear record assigning responsibility for implementing remedial actions or managing security risks; and
- have the results of security risk activity endorsed by the organisation's senior management.

2.6 The Gallery was the only organisation that had undertaken an organisation-wide review to identify and assess its security risks. The Gallery completed a comprehensive review of its security risks in March 2005.[18] The review assessed the risks and controls in place across each of the dimensions of protective security, including the risks associated with the Gallery's security awareness and training activities. To address shortcomings identified during the review, the Gallery implemented the following improvements to its security awareness and training arrangements:

- introduced a requirement for all security cleared staff to provide an annual acknowledgement of their responsibilities;
- updated its security policy and security awareness briefings to better promote the importance of reporting security incidents; and
- developed a more structured approach to security awareness training for non-security staff.

2.7 Archives and Health periodically undertake security risk reviews at their respective operational sites or locations.[19] These reviews largely focus on physical security issues, such as:

- use of closed circuit television and alarm systems and attendant monitoring arrangements;
- use of security containers;

[18] The Gallery undertook further assessments of its security risks in October 2007 and October 2008. The ANAO considered that these reviews, although not as broadly-based as the 2005 review, further improved the Gallery's understanding of its security risks, including the risks associated with security awareness.

[19] At the time of the audit, Archives had not undertaken a security risk review of its national office site in the ACT.

- procedures for disposing of sensitive and classified waste; and
- perimeter security issues, including access controls.[20]

2.8 The ANAO's examination of a sample of the site reviews undertaken by Archives and Health indicates that the approaches taken are not sufficient to satisfy the structured security risk management process recommended in Part B of the PSM. In particular, neither organisation maintained a consolidated record, nor was there any evidence of management's endorsement, of the security risks or issues identified during the reviews, or the actions taken in response. In addition, it was noted that while the reviews undertaken at Health addressed risks and issues associated with security awareness and training activities, the reviews at Archives did not.

2.9 In May 2009, an internal audit indicated that CrimTrac had not undertaken security risk assessments (and did not have security risk management plans) for its key ICT systems. At the time of the audit, CrimTrac advised that it was upgrading the security accreditation[21] of its ICT systems. CrimTrac further advised that this involves conducting an organisation-wide security risk assessment and the preparation of a security risk management plan. To support the project CrimTrac developed a detailed work plan identifying, and allocating responsibility (and timeframes) for, some 140 related tasks, including tasks related to the assessment of its ICT security risks.

2.10 The absence of an organisation-wide approach, including the maintenance of a sufficient level of documentation of the results (such as a security risk register), can undermine the effectiveness of security risk management processes. In addition, it increases the likelihood that security risks and issues faced by the organisation are not adequately factored into security awareness and training activities. This matter is explored further in Chapter 3.

2.11 Overall, the results of the audit indicate there is scope to improve the approaches the audited organisations use to identify and assess their security

[20] Both organisations also conduct specialised ICT security risk reviews. These processes were not examined as part of this audit.

[21] The security accreditation of ICT systems is the process by which an authoritative body accepts and gives approval that the residual risks relating to the operation of an information system are appropriate. The accreditation process involves assessing whether there are sufficient security measures, policies and procedures in place to protect the information that is processed, stored or communicated by that system. Refer to <http://www.dsd.gov.au/_lib/pdf_doc/ism/ISM> [accessed 24 November 2009].

risks. This finding is similar to that in ANAO's Audit Report No.44 2008-09. That report recommended 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.[22]

Recommendation No.1

2.12 The ANAO recommends that organisations assess their approach to the identification, analysis and monitoring of security risks against the guidance contained in Part B of the *Protective Security Manual*.

Organisations' responses to Recommendation No.1

Attorney-General's Department

2.13 Agreed. AGD recommends that agencies familiarise themselves with the International Standard on Risk Management (ISO 31000) and the Standards Australia Handbook *Risk Management Guidelines* (HB 435:2004) to assist in their assessment of agency specific risk.

CrimTrac

2.14 Agree. CrimTrac acknowledge the importance and immediate need to conduct a complete review on our security risk profile in accordance with Part B of the Protective Security Manual. CrimTrac believe that our security risk posture is correct and consistent with the PSM and the current threat landscape, but acknowledge the necessity to validate our protective security controls are effective.

2.15 CrimTrac have added this task to the work plan of the Protective Security and Property Manager who is currently being recruited. This important work has been flagged as an operational priority with the agency executive management team and has been recorded with the CrimTrac Audit Committee as an outstanding activity to ensure accountability and transparency of the associated rectification of this audit finding.

[22] ANAO, op. cit., p. 43.

Department of Health and Ageing

2.16 Agreed. The physical security site survey framework has been expanded to provide more detail as recommended. A more systematic and coordinated physical security risk management process is being adopted.

National Archives of Australia

2.17 The Archives agrees with ANAO recommendation No.1 and is developing a security policy, security risk plan and a security risk register that will establish the Archives' arrangements for the identification, analysis and monitoring of security risk in accordance with Part B of the Protective Security Manual.

National Gallery of Australia

2.18 Agree.

Security policies have been promulgated and are current

2.19 Clear, current and easily accessible security policies, together with related procedural documentation, are important to support managers and their staff in the performance of their functions. In particular, clear policies can assist staff to better understand the organisation's security risks, issues, and standards, as well as their own security related responsibilities. A security policy is also an appropriate method to communicate the importance of, and the organisation's commitment to, protective security, including security awareness and training activities.

2.20 Each of the audited organisations had a range of readily accessible security policy and procedural documents. The documents were generally comprehensive, dealing with relevant security issues and requirements in an informative manner. Importantly, the security policy documents at the Gallery and Health had been recently reviewed and endorsed by their respective senior management.

2.21 As well as describing the organisation's security environment, identifying key security roles and responsibilities and outlining the organisation's approach to managing security risks, the security policy documents at the Gallery and Health contain information on a wide range of pertinent security issues, including:

- physical security – such as perimeter and work area security, access controls, passes, clear desk policy and the use of storage containers;

- information security – explaining the 'need-to-know' principle, as well as procedures for classifying, handling and disposing of information;
- ICT security – providing information on the range of controls, management processes, supporting guidelines and technical standards associated with the use of ICT;[23]
- personnel security – information on undertaking and managing security clearances;
- how to report and manage security incidents; and
- in the case of the Gallery - details of its fire protection and artwork security arrangements, both of which are critical issues to the Gallery's operations.

2.22 The security policy documents at the Gallery and Health also contain information on the importance of security awareness and training and outline key elements of each organisation's security awareness program. For example, Health's policy document states 'security is a shared responsibility and security awareness is a key factor in promoting a security culture within the department'.

2.23 Archives and CrimTrac also have a range of security policy and procedural documents. Several of these documents were more than five years old at the time of the audit, and there was no evidence that they have been formally reviewed or updated since being released. There is an increased risk that outdated documents will not reflect the organisation's operating environment, including its key security risks and issues. In addition, these documents are unlikely to accurately reflect relevant requirements from the PSM and the ISM, as both manuals have been updated over that period.[24]

2.24 There would be benefit in the Archives and CrimTrac reviewing the currency of their security policy and procedural documents, including assessing whether they are consistent with the relevant standards in the PSM and the ISM. CrimTrac advised that a review (and update) of its security

[23] The security policy documents at both organisations contain references to more detailed documents addressing ICT security issues. These documents were not examined as part of the audit.

[24] For example, the version of the PSM published in October 2005 followed a major revision of protective security policy and requirements. The former ASCI 33 was updated and re-released every six months. The update released in March 2006 followed a major review of ICT security policy and requirements.

policies will occur as part of the project to update the security accreditation of its ICT systems.

Communication with senior management

2.25 Strong direction, leadership and commitment from an organisation's senior management are important to achieve and maintain effective protective security outcomes. As noted in ANAO's Audit Report No.44 2008–09, organisations should have regular communication lines to support senior managers to obtain sufficient understanding and assurance about security related matters.[25]

2.26 An important element in the involvement of senior management is the appointment of a Security Executive.[26] Each of the audited organisations had designated a member of their senior management to be the Security Executive, and in each case, the ANAO considered the position chosen to be appropriate. In addition, the ANAO observed that each Security Executive maintained regular contact (both formally and informally) with the organisation's security team.

2.27 Another way to support senior management is to regularly provide information on the status or performance of protective security issues. CrimTrac, the Gallery and Health each had formal and regular processes for communicating security related issues to senior management. For example, CrimTrac's Security Manager provides a *Security Report* to CrimTrac's Senior Executive each month. Among other things, these reports include details of current protective security (including ICT security) initiatives; and a range of statistics, including: intrusion attempts, and Email and Internet usage.

2.28 The ANAO considers that there would be merit in the Archives also reporting periodically on the status or performance of its protective security activities to its senior management.

2.29 Health was the only audited organisation to have established a security committee (known as the Risk and Security Committee) to support its Security Executive in the oversight, control and promotion of protective security

[25] ANAO, op. cit., p. 35.

[26] Defined in the PSM as a member of the Senior Executive Service that is responsible for the ongoing development of an organisation's security policy and the oversight of protective security matters within the organisation. (PSM, Part A, paragraph 4.10)

activities. The committee regularly reports to Health's Executive Committee on:

- the status of key security related business improvement projects;
- ICT security activities;
- security incidents; and
- a range of security related operational metrics (including security clearance workload measures).

2.30 Organisations should consider establishing a security committee, where it is cost effective to do so. In smaller organisations, the role of a security committee can be incorporated into an existing senior management committee, such as the audit committee.

Security awareness and training planning

2.31 Planning can assist an organisation develop coordinated and targeted security awareness and training programs, and help ensure that activities are designed to suit the roles and responsibilities of staff. The form and extent of planning required by each organisation depends on the organisation's circumstances, including its size, the nature of operations and its security risk profile.

2.32 A key element in the development of a security awareness and training plan is to conduct a gap analysis to identify:

- what security awareness and training risks exist;
- what awareness and training activities are needed, including the qualifications required by key security personnel;
- what is currently being done to meet those risks and needs; and
- the priorities for the treatments and strategies to address the risks and needs.

2.33 Figure 2 outlines the information often addressed in a security awareness and training plan.

Figure 2

Suggested content of a security awareness and training plan

- Reference to the policy requirements in the PSM and ISM
- Scope of the organisation's security awareness and training program
- Objectives of the overall program, and each major activity
- Intended benefits of the program, and each major activity
- Key roles and responsibilities, including identification of those personnel that will develop and maintain the security awareness and training material
- Methods to be used to promote security awareness
- Details of the security awareness training program, including arrangements for induction and refresher sessions, as well as additional specialised (tailored) streams
- Frequency (and location) of security awareness briefings or training
- Intended audience for each category of security awareness briefing or training
- Tools to obtain feedback about the methods used to promote security awareness, including briefing and training sessions
- Approaches used to measure and evaluate the effectiveness of the program

Source: ANAO.

2.34 Health, the largest of the audited organisations, was the only organisation that had an approved security awareness and training plan in place. Specifically the plan outlines the strategies developed by the department to enhance its approach to security awareness and training. These strategies include:

- developing a holistic and integrated approach to security awareness;
- undertaking targeted audience assessments;
- ensuring target audiences receive appropriate training;
- making effective use of communication channels; and
- monitoring and evaluating the impacts of the plan.

2.35 As well as these strategies, the plan outlines the:

- Australian Government's requirements, and the organisation's business imperative, for promoting and maintaining security awareness;
- key objectives of the plan and the associated roles and responsibilities;

- key dependencies to deliver the plan;
- measures of success; and
- range of security awareness activities employed by the department, including the mediums used and planned frequency of delivery.

2.36 CrimTrac advised that it had started to develop a formal ICT security awareness and training plan as part of the project to upgrade the security accreditation of its ICT systems. An early draft of the plan examined by the ANAO states that it will be designed to 'define the ICT security training and awareness services for those personnel responsible for the provision and maintenance of CrimTrac's Information Systems'.[27]

Implementation of relevant recommendation from previous ANAO audit

2.37 Audit Report No.55 2003–04, reported that none of the four audited organisations had formal plans in place to set out the direction of their security awareness activities. Accordingly, the Audit Report recommended:[28]

> Recommendation No.2: The ANAO **recommends** that organisations develop and implement a structured and proactive security awareness education and training strategy.

2.38 Health was the only organisation that had implemented the previous recommendation relating to the development of a structured security awareness plan or strategy. CrimTrac was assessed as partly implementing the recommendation.

2.39 The lack of planning of security awareness and training activities identified in this audit is consistent with the results in previous ANAO protective security audits. Thoughtful planning can contribute to the development of a more coordinated and targeted security awareness and training program, as well as help to achieve better outcomes.

---

[27] CrimTrac Agency, *Draft IT Security Training and Awareness Plan*, August 2008.

[28] ANAO, Audit Report No.55, *Management of Protective Security*, p. 33. Available at: <www.anao.gov.au/director/publications/auditreports.cfm>.

Recommendation No.2

2.40 The ANAO recommends that Australian Government organisations develop a security awareness and training plan that is commensurate with the organisation's circumstances, including its size and security risk profile, and that reflects the relevant requirements in the *Protective Security Manual* and the *Information Security Manual*.

Organisations' responses to Recommendation No.2

Attorney-General's Department

2.41 Agreed.

CrimTrac

2.42 Agree. CrimTrac have implemented a formal Security Awareness and Training plan for the agency. The implemented security awareness and training program addresses all recommended areas within the PSM and has been developed to complement CrimTrac's business and cultural drivers. The current training program has been provided for agency staff and contractors, currently eight staff (3 per cent) are awaiting training to bring the agency into 100 per cent compliance. This new program will be delivered monthly as an ongoing activity and staff will be required to undergo training on a yearly basis.

Department of Health and Ageing

2.43 Agreed. The Department will continue to implement the Security Awareness Plan and a small number of targeted presentations have recently been conducted.

National Archives of Australia

2.44 The Archives agrees with ANAO recommendation No.2 and is creating a security awareness and training plan and a security training handbook that is commensurate with our security risk environment. The plan will be informed by the conduct of security risk reviews at each of the Archives' facilities, security incident reports, the security risk register, and will be reviewed annually or as the security environment changes.

National Gallery of Australia

2.45 Agree.

3. Designing and Delivering Security Awareness and Training

This chapter examines the design and delivery of the audited organisations' security awareness and training activities.

Introduction

3.1 Shortcomings in security awareness and training can undermine the effective operation of the controls and practices that an organisation has put in place to manage exposure to its security risks. Accordingly, all people working in Australian Government organisations should be made aware of the main security risks faced by the organisation, [29] as well as the organisation's security policies, their roles and responsibilities in implementing those policies and the implications of poor security practices.

3.2 It is good practice to provide more targeted security training, briefings or guidance to those people involved in work areas or functions, including people that handle security-classified information, that are likely to be directly affected by the key security risks faced by the organisation.

3.3 In 2005, the Queensland Crime and Misconduct Commission identified 23 internal control areas, and a series of associated strategies, that are important for the effective management (and protection) of sensitive information.[30] One of these internal control areas was 'employee knowledge and understanding'.

3.4 The attendant strategies for this control included:

- adequately informing employees about the organisation's code of conduct, policies, practices, standards and guidelines;
- making employees aware of the importance of protecting sensitive information;

[29] PSM, Part B, paragraph 1.8.

[30] Queensland Crime and Misconduct Commission, *Information security: keeping sensitive information confidential* (Building Capacity series No. 7), February 2005, pp. 7-11. This publication is available from: <http://www.cmc.qld.gov.au/asp/index.asp?pgid=10818> [accessed 22 September 2009].

- clarifying employees' understanding of their protective security responsibilities;
- periodically reviewing levels of knowledge of security procedures; and
- clearly communicating any changes in security procedures to employees.

3.5 An organisation's security awareness and training program should promote an understanding of those requirements in the PSM and ISM that are pertinent to the roles and responsibilities of its staff. In this regard, the requirements in those manuals that are likely to have general application to the majority of Australian Government organisations include:

- understanding the organisation's security risks, including the roles and responsibilities for managing those risks;
- handling, storing and disposing of official information, including security classified information;
- determining the security classification of information, including the use of protective markings;
- responsibilities associated with holding a security clearance, including reporting any changes in circumstances;
- reporting details of security incidents;
- maintaining sound physical security policies and practices, including perimeter and work area access controls, the wearing of staff passes and the management of keys and combinations; and
- maintaining sound ICT security measures, including logical access requirements (such as passwords), media storage, managing software and network connectivity.

3.6 The PSM recognises that other legislation contains requirements relating to the protection of particular types of official information.[31] Accordingly, it is good practice for an organisation's security awareness program to also promote an understanding of any relevant 'confidentiality' obligations in legislation administered by, or affecting the organisation.

[31] PSM, Part C, paragraph 1.5.

3.7 In this part of the audit, the ANAO examined the design and delivery of security awareness and training activities. Specifically, we examined whether the audited organisations:

- used a variety of techniques or approaches to regularly promote security awareness;
- had security awareness and training programs that were sufficient and appropriate in light of:
  - the organisation's operations, including its security risks and issues;
  - selected security issues in the PSM;[32]
  - the requirements relating to the protection and confidentiality of information contained in the *Public Service Act 1999* (specifically in the APS Code of Conduct); and
- maintained sufficient records to substantiate the delivery of security awareness briefings and training.

3.8 As mentioned in Chapter 1, in examining the audited organisations' security awareness and training programs, we assessed the extent that Recommendation No.3 from ANAO Audit Report No.23 2002–03 *Physical Security Arrangements in Commonwealth Agencies* and Recommendation No.2 from ANAO Audit Report No.41 2007–08, *Management of Personnel Security Follow-up* have been implemented.

Security awareness techniques

3.9 Security awareness messages will be more effective when promoted and reinforced on a regular basis using a variety of mechanisms or tools. Organisations typically require a mix of general (organisation-wide) and targeted (role or work area specific) mechanisms; and use both active (such as briefings) and passive (such as posters) methods.

[32] The ANAO examined whether 17 security issues from the PSM were addressed in the audited organisations' security awareness and training activities. These issues were selected as they were considered likely to have general application to the majority of Australian Government organisations. Appendix 3 contains a list of the issues examined by the ANAO.

3.10 At a minimum, the ANAO expects organisations to promote an awareness of protective security as part of induction sessions for new starters. Depending on the significance of the security issues faced by the organisation, security awareness may also be reinforced through structured briefing or training sessions during the course of a staff member's employment. This is particularly important for those individuals with a security clearance. In addition, organisations should have a range of other mechanisms to help promote awareness and understanding of protective security issues, such as providing staff alerts on contemporary security issues and displaying posters containing security messages.

3.11 As shown in Table 3.1, for the most part, each of the audited organisations employed a good variety of techniques to regularly promote security awareness. Specifically, each of the audited organisations provided security awareness training as part of their induction process, as well as offering ongoing security awareness training or briefings. In addition, each of the audited organisations had processes in place to periodically communicate contemporary security issues to staff. On the other hand, only the Gallery and Health used posters or brochures to promote key security related messages.

Table 3.1

Techniques used by the audited organisations to promote security awareness

Technique	Archives	CrimTrac	Gallery	Health
a) Security awareness briefings or training provided as part of the organisation's induction process	✓	✗ [A]	✓	✓
b) Structured security awareness briefings or training (other than as part of induction processes)	✓	✓	✓	✓
c) Security clearance packs include information on the individual's ongoing security responsibilities	✓	✓	✓	✓
d) Posters or brochures highlighting key security messages are displayed around the workplace	✗	✗	✓	✓
e) Security issues are communicated to staff via Email alerts or in staff newsletters	✓	✓	✓	✓
f) An approved and up-to-date protective security policy (or series of policies) is readily available	✗ [B]	✗ [B]	✓	✓
g) Intranet contains guidance on protective security matters that is easy to locate, for example through a security home-page	✓	✓	✓	✓

Note A: Between April 2007 and March 2009, prior to the commencement of the audit, CrimTrac was using the Internet-based security training program developed by the Attorney-General's Department as part of its security awareness activities. CrimTrac discontinued use of this program on the basis that the program's content was not adequately meeting its requirements. Refer to further discussion at paragraphs 3.17 to 3.19.

Note B: As discussed in Chapter 2, at the time of the audit, several of the security policy and procedural documents at the Archives and CrimTrac were more than five years old.

Source: ANAO, based on fieldwork.

3.12 As well as the techniques outlined in Table 3.1, the ANAO identified a range of other beneficial security awareness techniques that were being used by one or more of the audited organisations. Table 3.2 sets out some of these practices.

Table 3.2

Additional security awareness techniques identified

Description of technique
All new starters at the Archives are required to sign a *Safeguard of Official Information* form. The form requires employees to acknowledge they have been made aware of the requirements in the *Public Service Act 1999* (and supporting regulations) and in the *Crimes Act 1914* dealing with protection of official information.
CrimTrac advised that members of its security team regularly visit work areas around the organisation to identify potential security issues and provide informal security briefings, and also periodically provide updates on ICT security at the organisation's monthly staff forums.
The Gallery requires all security cleared staff to acknowledge (annually) that they understand the obligations associated with having a security clearance, including the requirements associated with the classification and safeguarding of information.
The Gallery and Health both introduced online training and development programs (e-learning) during 2009. Health has encouraged all staff to complete the program, while the Gallery's program forms part of its new starter induction process. Both organisations' programs contain modules dealing with security issues, including ICT security. These programs each provide a range of information that is useful, relevant and well-targeted to the respective organisations' security environment.
Health's legal unit provides training on the requirements of the *Privacy Act 1988*, which includes advice on protecting the confidentiality of information, as well as training on the administration of the *Aged Care Act 1997,* which includes advice on the requirements (in that Act) relating to the protection of information.
Health has developed a series of factsheets on selected security issues, including: accessing the organisation's premises, classifying information, escorting visitors, clear desk policy, handling classified information, security roles and responsibilities, the use of security containers and reporting security incidents.

Source: ANAO, based on audit fieldwork.

Sufficiency and appropriateness of the content of security awareness and training programs

3.13 The design of an organisation's security awareness and training program should be tailored to reflect the organisation's circumstances and should be commensurate with the nature of the organisation's operations, including its security risks and issues.

3.14 As indicated in paragraph 3.7, the ANAO planned to examine whether the design (and content) of security awareness and training programs was sufficient and appropriate in light of each organisation's operations, including its security risks and issues. However, as discussed in Chapter 2 of this report, apart from the Gallery, none of the audited organisations had undertaken an organisation-wide review to identify and assess their security risks, nor did they maintain sufficient documentation of their security risks. As a result, the

organisations could not clearly demonstrate to the ANAO that details of their security risks were appropriately factored into the design of their security awareness and training programs.

3.15 Consequently, to assess the sufficiency and appropriateness of the organisations' security awareness and training programs, the ANAO examined whether the programs reflected the:

- nature of the organisation's information holdings, including the level of security classified and sensitive information;
- number of staff with security clearances;
- location, nature and value of physical assets;
- number of the organisation's operational sites; and
- existence of any specific requirements relating to the protection and confidentiality of information in legislation or agreements administered by the organisation.

3.16 The ANAO also examined whether the design (and content) of the audited organisations' security awareness and training programs was sufficient and appropriate in terms of selected issues from the PSM, as well as the requirements relating to the protection and confidentiality of information contained in the *Public Service Act 1999*.

3.17 As discussed in Chapter 2, at the time of the audit CrimTrac's security policy document was more than five years old, and there was no evidence that it had been formally reviewed or updated since being released. CrimTrac advised that it plans to review, and update as necessary, its security policy document. The ANAO did not assess the content of CrimTrac's security policy document as it intends to replace it.

3.18 As highlighted in Table 3.1, in March 2009 CrimTrac discontinued use of the AGD's Internet-based security awareness training program on the basis that the program's content was not adequately meeting its requirements. During the audit, CrimTrac was re-assessing its approach to security awareness training, including the development of training material more targeted to its security issues, including ICT security. As a result, it did not have a structured security awareness training program in place at the time of the audit. The ANAO did not assess the content of the security awareness training material as it is no longer being used by CrimTrac.

3.19 Since the cessation of the Internet-based training program, CrimTrac advised that it had initiated several measures to help inform staff of contemporary security issues. These measures included security personnel visiting work areas to identify potential issues and provide informal security briefings. CrimTrac did not have any evidence on the content (or the frequency) of these briefings.

3.20 Accordingly, the remainder of the discussion under the heading 'Sufficiency and appropriateness of the content of security awareness and training programs' is limited to the results of the ANAO's examination at the other three audited organisations.

3.21 As summarised in Table 3.3, the ANAO assessed that the content of security awareness and training material at the Archives, the Gallery and Health was, for the most part, sufficient and appropriate in terms of the elements examined.

Table 3.3

Assessment of the sufficiency and appropriateness of security awareness and training programs

Sufficient and appropriate in terms of…	Archives	Gallery	Health
Organisation's operating environment (based on the five factors listed in paragraph 3.15)	Partially	Substantially	Substantially
Selected security issues from the PSM[A]	Substantially	Substantially[B]	Fully
General requirements relating to the protection and confidentiality of information contained in the *Public Service Act 1999*	Partially	Substantially	Substantially

Notes:

A. The results of testing against the 17 selected issues are shown at Appendix 3.

B. Many of the selected security issues were only addressed in the Gallery's security policy document and not in its security awareness training material. Refer to further discussion at paragraph 3.30.

Source: ANAO, based on fieldwork.

3.22 The ANAO assessed that the design (and content) of the security awareness and training material at these organisations adequately reflected the nature of each organisation's information holdings and the value of physical assets. In addition, the design of the security awareness and training programs

at the Archives and Health reflect the fact that these organisations both have numerous operational sites.

3.23 The ANAO's examination also indicated that the organisations' security awareness and training programs largely addressed the selected issues from the PSM, and that the programs at the Gallery and Health adequately reflected the requirements for the protection of information contained in the *Public Service Act 1999*. As mentioned in Table 3.2, all new starters at the Archives are required to sign a *Safeguard of Official Information* form to acknowledge they have been made aware of the requirements in the *Public Service Act 1999* relating to the protection of information. The audit found that 67 per cent of 90 personnel files examined did not contain the acknowledgement form. Accordingly, the ANAO considers that this practice cannot be relied upon to have promoted a sufficient level of understanding of these requirements.

3.24 The ANAO also identified a number of opportunities to further improve the sufficiency and appropriateness of the audited organisations' security awareness training. In particular, improvements are needed to better address relevant security risks and issues. These opportunities are discussed in the following paragraphs.

Training staff with security clearances

3.25 At the time of the audit, a significant proportion of staff in each of the audited organisations held a security clearance. It is important that security cleared staff are provided with periodic and targeted training, briefings or other guidance to help them understand (and accept) the additional responsibilities associated with access to, and the management of security classified resources. Such targeted activity can also assist in the ongoing management of security clearances by providing an opportunity to identify issues impacting on the continued suitability of staff to hold a security clearance.[33]

3.26 The security awareness programs at each of the audited organisations provided information on the importance of security clearances, including details of the different types of clearances, the reasons for, and the processes to

[33] ANAO, Audit Report No.41 2007–08, *Management of Personnel Security – Follow Up, p. 70.* Available at: <www.anao.gov.au/director/publications/auditreports.cfm>.

obtain a security clearance. In addition, each of the audited organisations provided a range of general information to people, including those with a security clearance, on classifying, storing and disposing of security classified information.

3.27 However, with the exception of the annual acknowledgement form used by the Gallery, none of the audited organisations provided any training, briefings or had additional guidance targeted at the roles or responsibilities of security cleared staff. The annual acknowledgement form used by the Gallery is a sound method of reminding security cleared staff of their responsibilities.[34] Nevertheless, the Gallery would benefit from some additional tailoring of the form to better reflect the particular responsibilities, and the associated security risks of the different positions and work areas.

3.28 Health's security awareness plan states that the department intends to develop awareness information sessions targeted at security cleared staff. The plan indicates that these sessions will provide 'detailed guidance on the protection of security classified information'.

Addressing the organisation's security policies and procedures

3.29 Highlighting an organisation's security policies and procedural documents in security awareness training material reaffirms their importance. Furthermore, doing so provides an opportunity to assess and improve the levels of understanding (and the use) of the policy documents.

3.30 The Archives' ICT security awareness presentation and the ICT security briefings provided to new starters at the Gallery both contain references to the organisations' ICT security policy documents. However, the remaining security awareness training material used by these organisations does not contain any information on, or reference to, the organisations' key security policy and procedural documents. At the Gallery, the importance of including such references is underlined by the fact (highlighted in Table 3.3) that many of the selected issues from the PSM, while addressed in its security policy document, are not addressed in its security awareness training material.

3.31 In addition, the audit identified opportunities at the Archives and the Gallery to expand the scope of security awareness training material to better

[34] ANAO's examination of the personal security files of a sample of the Gallery's security cleared staff confirmed that these acknowledgement forms were being requested (and provided) in a timely manner.

reflect their respective security policies. For example, the Gallery's annual security awareness training session for non-security staff is predominantly focused on emergency management practices. While this is an important issue for the Gallery, there would be benefit in expanding the scope of these training sessions to address the Gallery's other key security policies. Depending on the audience, these briefings could include information on:

- access control arrangements;
- handling and storing sensitive and security classified material;
- close of business security procedures, including clear desk arrangements;
- reporting suspicious behaviour and security incidents;
- security of the exhibitions; and
- ICT security issues.

3.32 The Archives' (non ICT) security awareness training presentations contain information on access control arrangements and the use of storage containers, both of which are key security issues at the Archives. Notwithstanding the inclusion of this information, the ANAO assessed that the training material was too generic. There would be benefit in the Archives assessing whether its (non ICT) security awareness training material can be tailored to include more information on its key security issues and policies. For example, the relatively general discussion on security clearances in the presentations would be enhanced by including details of the Archives' security clearance requirements contained in the *Security Clearance and Access Policy.*

Referring to other relevant legislative requirements relating to the protection of information

3.33 It is good practice for an organisation's security awareness training program to contain information on any requirements in the organisation's enabling legislation, or in other legislation or agreements administered by, or affecting the organisation, that are designed to protect the confidentiality of particular information. This is particularly relevant when such requirements have broad application across the organisation. On the other hand, where the impact of such requirements is limited to certain work areas, these issues can generally be effectively addressed through each work area's business processes.

3.34 The *Archives Act 1983* contains a range of provisions relating to the protection of information including, section 30A (census information), Division 3 of Part V (access to Commonwealth records) and Part VII (care of the Archives' material). Despite the broad relevance of these provisions, none of the Archives' security awareness training material examined by the ANAO contained information on, or references to, these requirements. To help ensure that the staff dealing with these requirements have an appropriate level of knowledge and understanding, there would be benefit in Archives' tailoring its security awareness training program to include advice on these requirements, and on any relevant policies and practices.

Implementation of relevant recommendations from previous ANAO audits

3.35 Audit Report No.23 2002–03, observed that four of the seven audited organisations did not provide new starters with security awareness training. In addition, the level of ongoing security training for non-security staff in five of the organisations audited was insufficient. Accordingly, the Audit Report recommended:[35]

> Recommendation No.3: The ANAO **recommends** that agencies develop and schedule periodic formal education and awareness programs for non-security personnel addressing agency security standards.

3.36 Audit Report No.41 2007–08, reported that only two of the four audited organisations included advice on security aftercare[36] arrangements in security awareness activities, including reinforcing the importance of security cleared staff reporting any changes in their circumstances. Accordingly, the Audit Report recommended:[37]

> Recommendation No.2: The ANAO **recommends** that organisations promote security aftercare arrangements in security education and training activities.

3.37 The Archives, Gallery and Health were assessed as having implemented Recommendation No.3 from Audit Report No.23 2002–03.

---

[35] ANAO, Audit Report No.23 2002–03, *Physical Security Arrangements in Commonwealth Agencies*, p. 49. Available at: <www.anao.gov.au/director/publications/auditreports.cfm>.

[36] The term 'security aftercare' describes the practices used in the timely identification, and assessment, of issues relevant to an individual's ongoing suitability to hold a security clearance.

[37] ANAO, Audit Report No.41 2007–08, op.cit., p. 79.

CrimTrac, which was re-assessing its approach to security awareness training and did not have a structured security awareness training program at the time of the audit, was assessed as partly implementing the recommendation.

3.38 The Archives and Health were assessed as implementing Recommendation No.2 from Audit Report No.41 2007–08, as they both include information on security aftercare arrangements in security awareness training. The Gallery was assessed as partly implementing the recommendation as it promotes the requirement for security cleared staff to advise the Security Manager of any changes in their circumstances in the annual acknowledgement form. CrimTrac was assessed as not having implemented this recommendation as it does not promote security aftercare arrangements in security awareness training.

3.39 The results in this part of the audit indicate that the security awareness and training programs at the Archives, the Gallery and Health are, for the most part, sufficient and appropriate in terms of the factors examined. Nevertheless, as discussed in paragraphs 3.25 to 3.34 the audit did identify some opportunities to better target security awareness training activities. Specifically, there is scope for the audited organisations to further tailor the design of their security awareness training activities to address the security risks and issues that are relevant to them.

Recommendation No.3

3.40 The ANAO recommends that organisations' security awareness training programs are tailored to reflect the organisation's security risks and issues. This includes, as appropriate, having training on:

- the responsibilities of security cleared staff;
- the organisation's key security policies and procedures; and
- any requirements relating to the protection of information in legislation or agreements administered by, or affecting, the organisation.

Organisations' responses to Recommendation No.3

Attorney-General's Department

3.41 Agreed.

CrimTrac

3.42 Agree. The current CrimTrac Security Awareness and Training program will be re-evaluated after the rectification of recommendation one, with the aim of ensuring alignment of the training syllabus to the agency's current risk profile.

3.43 CrimTrac are developing a Security Awareness and Training program specifically tailored for staff with elevated security clearances or elevated system access with a specific focus on mandatory obligations in regards to the handling of material governed by security and privacy considerations. This program is scheduled for implementation by July 2010.

Department of Health and Ageing

3.44 Agreed. The Department needs to review its security awareness packages in relation to the specific legislation it either administers or is subject to.

National Archives of Australia

3.45 The Archives agrees with ANAO recommendation No.3. The development of the Archives' security awareness and training plan and the security training handbook includes responsibilities of staff and contractors who hold an Australian Government security clearance, the Archives' security policies and procedures, and applicable legislation for the handling of classified information and material.

National Gallery of Australia

3.46 Agree.

Maintaining sufficient records on the delivery of security awareness training

3.47 Maintaining accurate and complete attendance information can help organisations manage the scheduling and delivery of security awareness training. In particular, this information helps ensure that training is appropriate and timely, as well as being commensurate with staffs' roles and functions. Accurate attendance records also provide greater assurance to senior management that sufficient training has occurred.

3.48 The ANAO assessed whether the audited organisations maintained sufficient documentation to support the delivery of security awareness

training. The ANAO also examined available records to gauge the level of attendance at security awareness training at each of the audited organisations.

Assessing the nature of training records

3.49 The Gallery was the only organisation that maintained sufficient records of the delivery of, and attendance at, security awareness training. The recent introduction of e-learning applications at two of the organisations has resulted in the capture of more accurate and detailed information on the completion of security awareness training. There would be benefit in other organisations evaluating the cost-effectiveness of adopting an e-learning capability to, among other things, assist in the management of security awareness training records. Table 3.4 describes the nature of the security awareness training records observed at each of the audited organisations.

Table 3.4

Description of security awareness training records maintained by the audited organisations

Organisation	Details
Archives	Since February 2007, staff are required to acknowledge their attendance at Archives' induction training, which includes a session on security awareness. These attendance records are maintained in Archives' Human Resource Management Information System. The records relating to other security awareness trainings or briefings are unstructured. These records largely comprise a mix of signed and unsigned attendance sheets, and file notes or Emails stating that security training or a briefing session has been provided.
CrimTrac	During the period that it used the AGD's Internet-based security awareness training program, CrimTrac had access to a range of information enabling it to monitor completion of the program by its staff. CrimTrac does not maintain any structured records of the delivery of, or the level of attendance at, its other security awareness training activities. This includes the periodic informal security briefings and updates provided during the organisation's monthly staff forums.
Gallery	As part of the Gallery's induction process all new starters are required to obtain, using a 'post commencement checklist', written acknowledgement from the security area that they have been provided with a briefing on the Gallery's security requirements, as well as a copy of the 'security briefing handout'. The e-learning training program, introduced in April 2009, enables the Gallery to monitor a range of details, including the names of the staff that have completed the various training modules, the time spent on each module, and the number of questions answered correctly. The Gallery also maintains signed attendance records of the annual security training sessions provided to non-security staff.
Health	Prior to implementing its online training program in February 2009, Health did not maintain any formal records on the timing of, or the attendees at, security awareness briefings or training sessions.[A] Health advised that it monitors use of its online training package, in particular, details of total bookings and completion rates, which are included in monthly reports to its Chief Operating Officer.

Note A: As previously discussed, Health's security awareness plan indicates that the department intends to improve the maintenance of attendance records.

Source: ANAO, based on fieldwork.

Assessing the level of attendance at training

3.50 The lack of structured records at the audited organisations meant there was not always sufficient evidence to gain assurance that appropriate levels of security awareness training had occurred. As shown in Table 3.5, the records that were available suggest that the audited organisations can improve both the amount and the timeliness of security awareness training.

Table 3.5

Summary of attendance levels at security awareness training

Organisation	Details of attendance examined
Archives	Available records indicate only approximately 55 per cent of new starters at Archives since February 2007 have attended induction training. Of these, around 80 per cent attended induction training within six months of their commencement date, but only 16 per cent attended within two months, as required by Archives' policy. Available records indicate that between December 2003 and May 2009, Archives delivered nearly 50 security awareness briefing or training sessions (in addition to mandatory induction training) to a total of nearly 550 personnel. The records supporting the conduct of these security awareness briefings and training sessions are insufficient to enable the accurate identification of the attendees at each session.
CrimTrac	CrimTrac's records indicate that approximately 86 per cent of its current staff completed the AGD's online security awareness training program. Most of the staff who had not completed the training had commenced work at CrimTrac in the three months before the cessation of the arrangement. However, 10 per cent of the staff who had not completed the training had more than four years service with CrimTrac.
Gallery	ANAO's examination of the personnel files for 15 new starters at the Gallery in the period October 2008 to July 2009 indicates that 11 contained the 'post commencement checklist' showing that the new starter had been provided a security briefing and a copy of the 'security briefing handout'. ANAO's analysis indicates that only approximately 42 per cent of the Gallery's new starters between April and the end of September 2009 are recorded as having completed the e-learning induction program introduced in April 2009. In addition, a further 10 percent were recorded as having started (but not completed) the program. ANAO's examination indicates that around 40 per cent of staff were recorded as attending annual security training sessions in 2009. The Gallery's records indicate that over the last four years, on average, around 45 per cent of personnel have attended annual security refresher training.
Health	ANAO's examination indicates, at the end of August 2009, that only approximately 15 per cent of Health's staff had completed the online training program introduced in February 2009. In addition, approximately 30 per cent of staff are recorded as being 'booked' on the online training program.

Source: ANAO, based on fieldwork.

3.51 The results in this part of the audit indicate shortcomings in the level of record keeping relating to the delivery of security awareness training. By improving record keeping, organisations will be better placed to make sure that security awareness training is being provided in a timely manner. In addition, it will help improve their ability to manage attendance levels, including identifying individuals that have not attended training.

3.52 To improve the level of attendance at, or the completion of, security awareness training, there would also be benefit in organisations assessing the cost effectiveness of adjusting the format and timing of security awareness training. For example, attendance levels may be able to be improved by:

- offering staff greater flexibility regarding the availability of the training;
- incorporating security awareness training into other formal training programs, such as Occupational Health and Safety training; or
- tailoring training sessions to better suit particular work areas or staff groups within the organisation.

Recommendation No.4

3.53 To assist in the provision of appropriate and timely training, the ANAO recommends organisations maintain accurate and complete records of the delivery of, and attendees at, security awareness training.

Organisations' responses to Recommendation No.4

Attorney-General's Department

3.54 Agreed.

CrimTrac

3.55 Agree. CrimTrac have implemented this recommendation and maintain accurate and complete records of all deliveries and attendees for all security awareness training presentations, including a forward schedule addressing training re-certification.

Department of Health and Ageing

3.56 Agreed. More detailed records reflecting specific and generic training conducted and attendance records are now being kept by the Department.

National Archives of Australia

3.57 The Archives agrees with ANAO recommendation No.4 and has implemented an electronic record for all staff and contractors who participate in security training, either as part of an induction process, re-evaluation of a security clearance or an issue targeted session. The security team reports internally on the number of people who attend security training.

National Gallery of Australia

3.58 Agree.

4. Monitoring the Effectiveness of Security Awareness and Training

This chapter examines how the audited organisations assess the effectiveness of their security awareness and training activities.

Introduction

4.1 Organisations that regularly monitor and assess the effectiveness of security awareness and training activities are well placed to make timely improvements, as necessary, to the approaches they use. The information gained through monitoring can assist organisations to identify opportunities to improve the timing or focus of their security awareness activities, including by detecting delivery techniques that are not working well, or are no longer useful.

4.2 Organisations may assess whether:

- staff understand the key messages;
- there are any gaps in the information provided; and
- there have been any changes in awareness levels, attitudes and behaviour across the organisation.

4.3 In this part of the audit, the ANAO examined whether the audited organisations regularly monitor and report on the effectiveness of security awareness and training programs, including by analysing the level and impact of security breaches or incidents.

Monitoring the effectiveness of security awareness and training activities

4.4 None of the audited organisations had regular and structured processes in place to assess the impact and success (or otherwise) of their security awareness and training activities. As mentioned at paragraph 2.27, three of the audited organisations had regular processes for communicating security issues to senior management. However, this reporting did not include information on the effectiveness of their security awareness and training activities.

4.5 One of the key strategies in Health's security awareness plan is to monitor and evaluate the impact of the plan. In this regard Health identified the following potential measures of success:

- trends in responses to external security questionnaires and audits;
- levels of staff attendance at security awareness sessions;
- reductions in the number of security incidents;
- business processes being modified to comply with security requirements; and
- results of annual employee survey on security awareness and training.

4.6 Health advised that work had begun on developing the processes necessary to capture the information required for these measures. For example, Health plans to introduce sign-on forms to capture attendance details at future security awareness training sessions. In addition, at the time of the audit, a draft of the proposed employee security awareness survey had been developed.

4.7 The audited organisations did, however, use a range of intermittent processes to obtain information on security awareness levels. A summary of the various methods that the ANAO observed during the audit is provided below.

Monitoring security incidents

4.8 Security incidents can provide valuable insights into an organisation's security environment, including the level of security awareness. Common types of security incidents that may be indicative of security awareness issues include:

- loss of personal or official resources;
- unauthorised access to an organisation's premises or certain work areas;
- unauthorised release or transmission of information, particularly security classified information;
- incorrect storage of sensitive or security classified information;
- failure to lock security containers, including not securing the keys or combinations to those containers; and

- compromise of access controls, such as the loss or improper use of access cards or passwords.

4.9 Each of the audited organisations has implemented procedures to identify and capture details of security breaches or incidents. The ANAO reviewed a sample of security incidents at each organisation to assess if incidents bore evidence of timely action, and to identify the level of incidents that were indicative of security awareness issues. The results are shown in Table 4.1.

Table 4.1

Analysis of security incident records at the audited organisations

Organisation	Details
Archives	The ANAO examined a sample of 27 security incident reports over the period October 2008 to July 2009. The ANAO's examination indicated that incidents were clearly documented with follow-up action generally occurring in a timely manner.[A] The ANAO noted that 11 of the examined incidents related to security containers being left unsecured. The ANAO considers recurring incidents of this kind can indicate shortcomings in security awareness levels.
CrimTrac	During 2009, CrimTrac developed a spreadsheet to facilitate the recording and monitoring of security incidents. At the time of the audit no incidents had been recorded in the spreadsheet.[B]
Gallery	The ANAO reviewed the Gallery's register of security incidents for the 2008 and 2009 calendar years. The ANAO's examination indicated there was generally a good description of each incident, and of the action taken in response. The ANAO observed five incidents that potentially related to a shortcoming in security awareness. Each was resolved in a timely manner, with no indication of any loss or compromise of assets or information.
Health	The ANAO examined 13 weekly security incident reports over the period May to July 2009. For each recorded security incident there was a good description of the incident, as well as a record of the follow-up action. The ANAO considered that only two incidents were indicative of a lack of security awareness. In both cases, the matter was resolved in a timely manner and the follow-up action was considered to be appropriate.

Notes

A: The files containing security incident reports at the Archives were unstructured and individual reports and associated information were not filed in any consistent order (such as chronologically or numerically) or assigned a unique number (such as an incident number).

B: A recent internal audit report on physical security at CrimTrac observed that details of security incidents contained in a separate register (maintained by CrimTrac's contracted guards) were not being consolidated into the spreadsheet maintained by the security team. The ANAO did not examine the register maintained by CrimTrac's guards.

Source: ANAO.

4.10 Archives advised that it does not monitor trends in security incidents or actively use the results of security incidents to inform the design of its

security awareness activities. On the other hand, the Gallery and Health advised that details of security incidents are periodically monitored and used to inform the design of security awareness and training activities. The Gallery cited the following examples where a security incident prompted security awareness action:

- additional targeted briefings were delivered to security attendants to address incidents related to 'artwork touches'; and
- following an incident involving the improper use of a staff member's pass the Security Manager included information in the Gallery's staff bulletin highlighting the risks of doing so.

Internal audits

4.11 The PSM recommends that organisations conduct 'regular security audits to ensure that protective security measures are efficiently and effectively implemented'.[38] While the PSM is not prescriptive as to the scope of such audits, the ANAO considers it good practice to periodically evaluate the effectiveness of security awareness and training activities as part of any program of security audits.

4.12 None of the audited organisations had undertaken an internal audit that incorporated an examination of security awareness and training issues in the previous two years. However, a recent internal audit examining CrimTrac's physical security policies and procedures recommended that CrimTrac ensure that all employees are provided with training, and that regular reminders are issued on the requirements for managing security classified documents.

Focus groups

4.13 The use of targeted focus groups, or a well-designed survey or questionnaire, can be helpful in obtaining information from staff about their views on, and assessing their understanding of, security awareness and training issues. A list of potential questions that could be used in a survey is included at Appendix 4.

[38] PSM, Part A, paragraph 6.1.

4.14 In 2005–06, Health conducted a series of focus groups to assess the impact of its (then) security awareness communication initiatives. Among other things the focus groups were designed to:

- assess the impact of initiatives on staff security awareness levels;
- identify which security awareness activities were working to achieve the objectives of Health's (then) security awareness strategy;
- identify barriers to, and opportunities for, greater staff engagement and collaboration with the security team; and
- identify opportunities for improvement in the current range of security awareness activities.

4.15 The ANAO considers that this exercise was useful in providing Health with information to improve its security awareness activities. In particular, the research found that increased efforts (at that time) to promote security awareness had resulted in 'small gains' in security awareness levels. As noted in paragraph 4.6, at the time of the audit, Health plans to undertake another staff survey to assess security awareness levels.

4.16 Overall, the results of the audit indicate that the audited organisations can improve the level of monitoring they undertake of the effectiveness of their security awareness activities. Each organisation needs to find the right balance in assessing the effectiveness of its security awareness and training activities, as there is no 'one size fits all' solution. The approach taken should be cost-effective and not overly onerous. The following measures can be useful to assess the effectiveness of security awareness activities:

- reviewing security incidents to identify those potentially relating to a lack of, or breakdowns in, security awareness;
- periodically examining security awareness issues in internal audits or other management reviews or assessments;
- periodically conducting focus groups, or undertaking surveys, to obtain information on the level of security awareness in the organisation; and

- monitoring the number of hits on security awareness resources contained on the organisation's Intranet.[39]

Recommendation No.5

4.17 The ANAO recommends that organisations implement cost-effective arrangements to periodically monitor the effectiveness of their security awareness and training activities.

Organisations' responses to Recommendation No.5

Attorney-General's Department

4.18 Agreed.

CrimTrac

4.19 Agree. CrimTrac acknowledge the importance of validating the success of its security awareness and training program and have recorded this recommendation into our business work plan. The following activities will be implemented to measure the success of our training program:

- formal security breach program;
- security awareness training attendance reporting and analysis;
- single online security incident reporting capability (completed);
- online staff surveys;
- targeted informal security awareness sessions; and
- addition of protective security incident reporting in agency monthly security reports.

Department of Health and Ageing

4.20 Agreed. The Department is putting in place a more comprehensive framework to monitor the effectiveness of security awareness and training activities. The first staff survey of a number of Divisions has been completed. A similar survey of State and Territory Offices is currently underway and initial

[39] This list is based on the measures observed during the audit and information in the European Network and Information Security Agency (ENISA) study – *Information security awareness initiatives: Current practice and the measurement of success*, July 2007, p. 18. Available at: <http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf> [accessed 12 June 2009].

responses from a number of Offices have been received. Other avenues for monitoring the effectiveness of security awareness and training activities include; a structured program of awareness training, monitoring security incidents, internal audits and direct feedback from presentations.

National Archives of Australia

4.21 The Archives agrees with ANAO recommendation No.5. The security awareness and training plan, described above, includes metrics for the evaluation of the effectiveness of security awareness and training. The metrics include:

- the number of staff and contractors attending security training;
- the number of staff and contractors enquiring about security policies and procedures; and
- security incident statistics and analysis.

4.22 The above metrics and the effectiveness of the security training will be reviewed as part of the annual review of the Archives' security risk register.

National Gallery of Australia

4.23 Agree.

Ian McPhee
Auditor-General

Canberra ACT
15 April 2010

Appendices

Appendix 1: Audited organisations' responses to the proposed audit report

Each of the audited organisations, together with the Attorney-General's Department was invited to comment on the proposed audit report in accordance with the provision of section 19 of the *Auditor-General Act* 1997. In addition, the Department of Finance and Deregulation was invited to comment on an extract of the proposed audit report. Appendix 1 contains the comments received.

The organisations' responses to each of the recommendations have been included in the body of the report under the sub-heading 'Organisations' responses' directly following each recommendation.

Attorney-General's Department

The AGD welcomes the ANAO report *Security Awareness and Training*, noting that the report hopes to strengthen the security awareness and training regimes within the four audited agencies, and across Government.

AGD supports all recommendations outlined in this report.

AGD recognises the ANAO findings that although the status of security awareness and training was deemed to be adequate, there remains considerable scope for agencies to enhance the effectiveness of the programs in place, and in particular, through tailoring security awareness and training to better reflect agencies' specific security risks.

AGD notes the recognition of the steps taken to address the issue of applicability of the Protective Security Manual to bodies operating under the *Commonwealth Authorities and Companies Act 1997*, and agrees that the process of issuing a General Policy Order will commence once the review of protective security policy has been completed.

CrimTrac

The CrimTrac agency has undergone a rapid and unprecedented growth in the last two years and has invested heavily in its Protective and Information Security commitments. During this period of growth, CrimTrac have identified improvement opportunities which will enhance its capacity to deliver secure and accountable business solutions to the law enforcement communities of Australia. Over the last two years CrimTrac have developed a formal Security Management structure, including a dedicated team of specialists in the field of

Information, Personnel and Protective Security. This team has been empowered to implement and bring about reform within the agency and its current business processes to ensure compliance with Commonwealth guidelines. The ANAO findings are welcome and reaffirm the existing agency Strategic Security Plan, which had identified similar objectives, and improvement opportunities.

Department of Finance and Deregulation

Finance agrees with the extract to the proposed audit report.

Finance is currently consulting with departments regarding the creation of General Policy Orders for various existing Australian Government policies.

Department of Health and Ageing

The Department welcomes this report and agrees with each of the five recommendations.

National Archives of Australia

The Archives agrees with the findings of the proposed audit report and supports the recommendations made. The Archives has already begun to address a number of issues identified during the audit.

National Gallery of Australia

The NGA agrees with the five recommendations outlined in the report and notes that the protective security management systems in place at the Gallery, on the whole, meet the recommendations.

Appendix 2: Previous ANAO Protective Security Audit Reports

- 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*;
- 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*; and
- ANAO Audit Report No.44 2008–09, *Security Risk Management*.

Appendix 3: Assessment of the coverage of selected security issues in security awareness and training programs[A]

Description of security issue	Archives	Gallery	Health
An awareness of security risks and taking responsibility for managing security risks *(PSM, part B, paragraph 1.8)*	✓	✓	✓
Responsibilities in handling sensitive information *(PSM, Part C, paragraphs 1.3, 1.14 and 3.15)*	✓	✓[B]	✓
Information should only be made available to people who have a legitimate 'need-to-know' to perform their official duties or contractual responsibilities *(PSM, Part C, paragraphs 1.3 and 6.10)*	✓	✓[B]	✓
Those with access to official information are aware of information security practices and standards, and, where applicable, hold an appropriate security clearance *(PSM, Part C, paragraph 3.12)*	✓	✓[B]	✓
Employees hold an appropriate security clearance and are aware of the appropriate protective security procedures for handling official information, especially security classified information *(PSM, Part C, paragraph 3.14)*	✓	✓[B]	✓
Awareness and details of where to locate the organisation's security policy (or policies) *(PSM, Part C, paragraph 4.3)*	✗[C]	✗[C]	✓
The ICT security measures to be adopted to protect the integrity and availability of information, as well as its confidentiality *(PSM, Part C, paragraph 4.18)*	✓	✓	✓
How to determine the appropriate security classification to be placed on information *(PSM, Part C, Paragraphs 6.12 and 6.31 to 6.86)*	✓	✓[A]	✓
The use of protective markings *(PSM, Part C, Paragraphs 6.5 and 6.28)*	✓	✗	✓
Close of business standards (clear desk requirements) *(PSM, Part C, paragraph 7.8)*	✓	✓[B]	✓

Description of security issue	Archives	Gallery	Health
Storage of classified information *(PSM, Part C, paragraphs 6.11 and 7.42)*	✓	✓[B]	✓
Handling, use and destruction of official information *(PSM, Part C, paragraphs 7.25 to 7.62 and 7.80 to 7.97)*	✓	✓[B]	✓
Notifying the entity about changes in personal circumstances *(PSM, Part D, paragraph 10.26)*	✓	✓[D]	✓
Issues associated with home-based work *(PSM Part A, paragraph 2.9 and Part H, paragraphs 3.6 to 3.7)*	✗	✓[B]	✓[E]
Physical security related responsibilities and obligations *(PSM, Part E, paragraph 3.13)*	✓	✓	✓
Security issues associated with the processing, storage and communication of official information using ICT systems *(PSM, Part C, paragraphs 7.23 to 7.24)*	✓	✓	✓
Details of security incident reporting processes *(PSM, Part G, paragraph 3.6)*	✓[B]	✓	✓

Notes:

A. As noted at paragraphs 3.17 to 3.19, the content of CrimTrac's security awareness and training program was not assessed in terms of these elements.

B. These issues are addressed in the organisations' security policy documents, but are not covered in their security awareness training material.

C. As discussed in Chapter 3, the Archives' and the Gallery's ICT security awareness training material includes references to their respective ICT security policy documents. However, the organisations' other key security policy documents are not referred to in the organisations' remaining security awareness training material.

D. Addressed in the Gallery's annual acknowledgement of security clearance responsibilities.

E. Health's security policy document contains information on this issue, although it is not covered in security awareness training material. However, the training material includes information on how to find Health's security policy document.

Source: ANAO based on the PSM, October 2007.

Appendix 4: Sample security awareness staff questionnaire

The following questions may be useful to obtain preliminary information about the security awareness levels of staff in the organisation. The number (and nature) of questions used by an organisation will depend on its own circumstances, including the nature of its security risks and issues.

1) How would you describe your responsibilities relating to the protection of the organisation's official resources?

- ☐ I am responsible for assisting with the protection and proper use of the organisation's official resources
- ☐ I am required to have an understanding of the processes designed to protect the organisation's official resources
- ☐ I incorporate proper security practices into my day-to-day functions and activities
- ☐ All of the above

2) From a security perspective, when leaving your desk unattended, why are you required to lock your computer?

- ☐ It reduces the cost of Internet use
- ☐ It saves power
- ☐ It helps prevent unauthorised access to sensitive and security classified information
- ☐ It prevents other employees from using my Email account

3) The term 'Clear Desk Policy' means:

- ☐ All information, including electronic media are secured in appropriate containers when I am absent from my workstation
- ☐ As above, but only when I am away from my workstation for in excess of 2 hours
- ☐ That I should attempt to finish any outstanding work by the close of each day

4) Do you know where to find the organisation's security policy and procedural documents?

5) Do you know how to contact the organisation's agency security adviser and information technology security adviser?

6. Which of the following categories of security classifications should be used for information that could cause harm to Australia's national security?
   - ☐ Confidential, Protected, Sensitive or X-in-Confidence
   - ☐ Top Secret, Secret, Confidential or Restricted
   - ☐ Very Secret, Secret, Highly Protected or X-in-Confidence
   - ☐ Top Secret, Secret, Confidential or Highly Protected

7. Which of the following categories of security classifications should be used for information that could cause harm to any individual or organisation?
   - ☐ Secret, Confidential or X-in-Confidence
   - ☐ Secret, Restricted or Sensitive
   - ☐ Highly Protected, Protected or X-in-Confidence
   - ☐ Secret, Confidential or Highly Protected

8. If you hold a current 'Confidential' level of security clearance, what levels of security classified information can you access (provided you have a 'need-to-know')?
   - ☐ Highly Protected
   - ☐ Confidential
   - ☐ Protected
   - ☐ Secret

9. Do you consider the security home-page on the organisation's Intranet a useful source of information?

10. How would you rate the security arrangements in your immediate work area, including the level of security awareness.

11. Describe what you would do if you became aware of a potential security incident.

12. Have you changed your views, behaviour or attitudes in response to any of the organisation's security awareness measures (such as screen savers or the newsletter) or by attending security awareness training?

Source: ANAO, based on:

- Security Awareness Education and Motivation, *Measure What Matters,* Available at: <http://www.nativeintelligence.com/ni-programs/metrics-01.asp> [accessed 12 June 2009].
- Security Awareness questionnaire developed by the Department of Innovation, Industry, Science and Research; and
- Draft Security Awareness survey developed by the Department of Health and Ageing.

Index

Series Titles

ANAO Audit Report No.1 2009–10
Representations to the Department of the Treasury in Relation to Motor Dealer Financing Assistance
Department of the Treasury
Department of the Prime Minister and Cabinet

ANAO Report No.2 2009–10
Campaign Advertising Review 2008–09

ANAO Audit Report No.3 2009–10
Administration of Parliamentarians' Entitlements by the Department of Finance and Deregulation

ANAO Audit Report No.4 2009–10
The Management and Processing of Annual Leave

ANAO Audit Report No.5 2009–10
Protection of Residential Aged Care Bonds
Department of Health and Ageing

ANAO Audit Report No.6 2009–10
Confidentiality in Government Contracts – Senate order for Departmental and Agency Contracts (Calendar Year 2008 Compliance

ANAO Audit Report No.7 2009–10
Administration of Grants by the National Health and Medical Research Council

ANAO Audit Report No.8 2009–10
The Australian Taxation Office's Implementation of the Change Program: a strategic overview

ANAO Audit Report No.9 2009–10
Airservices Australia's Upper Airspace Management Contracts with the Solomon Islands Government
Airservices Australia
Department of Infrastructure, Transport, Regional Development and Local Government

ANAO Audit Report No.10 2009–10
Processing of Incoming International Air Passengers
Australian Customs and Border Protection Service

ANAO Audit Report No.11 2009–10
Garrison Support Services
Department of Defence

ANAO Audit Report No.12 2009–10
Administration of Youth Allowance
Department of Education, Employment and Workplace Relations
Centrelink

ANAO Audit Report No.13 2009–10
Major Projects Report 2008–09
Defence Materiel Organisation

ANAO Audit Report No.14 2009–10
Agencies' Contract Management
Australian Federal Police
Austrade
Department of Foreign Affairs and Trade

ANAO Audit Report No.15 2009–10
AusAID's Management of the Expanding Australian Aid Program
AusAID

ANAO Audit Report No.16 2009–10
Do Not Call Register
Australian Communications and Media Authority

ANAO Audit Report No.17 2009–10
Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2009

ANAO Audit Report No.18 2009–10
LPG Vehicle Scheme

ANAO Audit Report No.19 2009–10
Child Support Reforms: Stage One of the Child Support Scheme Reforms and Improving Compliance

ANAO Audit Report No.20 2009–10
The National Broadband Network Request for Proposal Process
Department of Broadband, Communications and the Digital Economy

ANAO Audit Report No.21 2009–10
Administration of the Water Smart Australia Program
Department of the Environment, Water, Heritage and the Arts
National Water Commission

ANAO Audit Report No.22 2009–10
Geoscience Australia

ANAO Audit Report No.23 2009–10
Illegal Foreign Fishing in Australia's Northern Waters
Australian Customs and Border Protection Service

ANAO Audit Report No.24 2009–10
Procurement of Explosive Ordnance for the Australian Defence Force
Department of Defence

Current Better Practice Guides

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

Innovation in the Public Sector	
Enabling Better Performance, Driving New Directions	Dec 2009
SAP ECC 6.0	
Security and Control	June 2009
Preparation of Financial Statements by Public Sector Entities	June 2009
Business Continuity Management	
Building resilience in public sector entities	June 2009
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
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
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
Controlling Performance and Outcomes	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997