The Auditor-General
Audit Report No.23 2002–03
Protective Security Audit

Physical Security Arrangements in Commonwealth Agencies

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 80679 9

Australian National
Audit Office

Canberra ACT
20 December 2002

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken a protective security audit 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 this report of this audit and the accompanying brochure. The report is titled *Physical Security Arrangements in Commonwealth Agencies.*

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

P. J. Barrett

P. J. Barrett
Auditor-General

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

AUDITING FOR AUSTRALIA

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

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

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

Telephone: **(02) 6203 7505**
Fax: **(02) 6203 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
Samantha Montenegro
Ben Sladic
Sonia Mercier
Richard Rundle

Contents

Abbreviations

ACSI	Australian Communications-Electronic Security Instruction
ANAO	Australian National Audit Office
APS	Australian Protective Service
ASA	Agency Security Adviser
ASP	Agency Security Plan
ASIO	Australian Security Intelligence Organisation
CPTED	Crime Prevention Through Environmental Design
DSD	Defence Signals Directorate
HBW	Home-Based Work
IT	Information Technology
ITSA	Information Technology Security Adviser
KPI	Key Performance Indicator
PSCC	Protective Security Coordination Centre
PSM	Protective Security Manual 2000
PSPC	Protective Security Policy Committee
PSRR	Protective Security Risk Review
SCEC	Security Construction and Equipment Committee
SEC	Security Equipment Catalogue
SID	Security-in-Depth
SOP	Standard Operating Procedure
SRA	Security Risk Assessment
SSP	Site Security Plan

Glossary

agency includes all Commonwealth Government departments, authorities, agencies, or other bodies established in relation to public purposes, including departments and authorities staffed under the *Public Service Act 1999*.

Agency Security Adviser the person nominated by the agency for the day-to-day performance of the protective security function within the agency.

Agency Security Plan the plan of action the agency intends to use to address its security risk based on the context in which the agency operates and a thorough risk review. It is one of the means by which an agency will demonstrate a commitment to general risk management.

clear desk policy a policy that dictates that people must ensure that security classified information and other valuable resources are secured appropriately when absent from the work place.

Crime Prevention Through Environmental Design a set of principles used to identify aspects of the physical environment that could affect people's behaviour, and that uses those aspects to minimise crime.

emergency management a range of measures designed to manage risks to agencies from disasters and emergencies. It involves developing and maintaining arrangements to prevent or mitigate, prepare for, respond to, and recover from emergencies and disasters.

incident reporting a scheme whereby security incidents (which can include security breaches, violations, contacts or approaches) are reported to a central point in the agency, usually the ASA. This enables the agency to collect statistics on its security vulnerabilities.

national security a term used to describe the safety of the nation from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference.

need-to-know principle the principle that the availability of official information should be limited to those who need to use or access the information to do their work.

physical security the part of protective security concerned with the provision and maintenance of a safe and secure environment for the protection of agency employees and clients, physical measures designed to prevent unauthorised access to official resources and to detect and respond to intruders.

protective security the total concept of information, personnel, physical and information technology and telecommunications security.

protective security audit an audit (or system of checking for compliance to predetermined standards) on the protective security arrangements in place in an agency.

Protective Security Coordination Centre a division of the Attorney- General’s Department responsible for developing protective security policy.

Protective Security Policy Committee a high-level interdepartmental consultative committee consisting of senior executives from agencies with a strong interest in national and non-national security matters.

risk exposure to an event which could result in loss or harm. Risk is measured in terms of vulnerability, event likelihood and event consequence.

risk analysis the systematic use of available information, based on the evaluation of likelihood and consequence, to determine risk.

risk management the systematic application of management policies, procedures and practices to the tasks of identifying, analysing, evaluating, treating and monitoring risk.

risk rating a rating that indicates how significant each identified potential risk is to an agency. The risk rating may be expressed a number of ways, for example, by using terms such as ‘severe’, ‘high’, ‘major’ and ‘significant’.

risk treatment selecting and implementing appropriate intervention strategies for dealing with risk.

security culture the ready acceptance by people that the securing of official information and other agency resources is an important and integral part of everyday work practices. The culture of a work group describes the patterns of basic assumptions, beliefs, customs and attitudes of the group which shape the behaviour of members of that group.

Security Equipment Catalogue a security classified guide for agencies issued by the SCEC on security items that have been endorsed by the SCEC or approved by ASIO for site-specific applications.

security incident a security breach, violation, contact or approach from those seeking unauthorised access to official resources, or any other occurrence that results in negative consequences for the Commonwealth.

security-in-depth principle a system of multiple layers, in which security countermeasures are combined to support and complement each other, making unauthorised access by an external intruder or employee with no need-to-know difficult; for example, physical barriers should complement and support procedural security measures and vice versa.

security risk a measure of potential loss or harm relevant to an agency's protective security arrangements.

Security Risk Assessment the process used to determine risk management priorities by evaluating risk against predetermined criteria, in the context of an agency's protective security arrangements.

security risk criteria statements that communicate the expectations of an agency's senior management about the agency's security environment. These criteria help an agency identify security risk and prepare appropriate security treatments, and provide a benchmark against which the success of the security plan can be measured.

Site Security Plan a plan that documents measures to reduce to an accepted level the identified risks to the agency's functions and resources at a designated site.

threat a source of harm that is deliberate or which has intent to do harm.

threat assessment evaluation and assessment of the intentions of people who could pose a hazard to a resource or function, how they might cause harm and their ability to carry out their intentions. Threats must be assessed to determine what potential exists for them to actually cause harm.

Summary and Recommendations

Summary

Background to the audit

1. Protective security involves the total concept of information, personnel, physical, information technology and telecommunications security. The Commonwealth's Protective Security Policy is outlined in the Protective Security Manual (PSM). It provides specific guidance to agencies on the protection of the Commonwealth's information, assets, personnel and clients from potential security threats.

2. Part E of the PSM outlines the Commonwealth's physical security policy, including the recommended physical security framework, procedures and minimum standards. Physical security is an essential component of the protective security framework for the identification, assessment and control of physical security risks.

3. Reviews of physical security in some State public sector organisations have identified deficiencies in their physical security arrangements. For example, a review conducted in 1996 by the Office of the Auditor-General of Western Australia[1] identified that many agencies were not: undertaking sufficiently comprehensive security risk assessments; developing adequate security policies and guidelines; implementing a comprehensive system for recording and monitoring security breaches; and defining, allocating and enforcing security responsibilities. These findings have some ongoing lessons for the Commonwealth.

4. In more recent years, the introduction of changed work practices such as an increasing reliance on information technology, contracting and home-based work practices exposes the Commonwealth to new vulnerabilities and risks. In addition, the international and domestic security events that have occurred over the past 15 months,[2] have given rise to a heightened awareness of the range of risks to be managed by Commonwealth agencies.

5. Such risks and vulnerabilities need to be understood, prioritised, and managed to prevent the occurrence of harm.[3] Agencies should keep in mind their obligation to provide a control environment that:

- limits the potential for the integrity, availability and confidentiality of official information and resources to be compromised; and
- adequately protects the safety of personnel and clients.

[1] Office of the Auditor-General of Western Australia, *Guarding the Gate—Physical Access Security Management within the Western Australian Public Sector*, Report No. 5—September 1996.

[2] For example, the terrorist attacks in the United States of America on 11 September 2001 and in Bali on 12 October 2002, as well as the recent shooting of the Director of the Mental Health Services, Human Services Department in Adelaide on 14 October 2002.

[3] The PSM defines harm to be any negative consequence, such as compromise of, or damage to, or loss incurred by, the Commonwealth.

Audit objectives and scope

6. This audit evaluated the protective security policies and practices of seven Commonwealth agencies to determine whether they had established an appropriate physical security control framework based on the principles outlined in the PSM. Specifically, the ANAO examined whether the agencies had:

- assigned roles and responsibilities for security;
- undertaken an appropriate Security Risk Assessment (SRA) process prior to developing the Agency Security Plan (ASP) and/or Site Security Plan (SSP);
- documented and implemented an effective set of controls and procedures to limit the impact and/or consequence of their identified security risks to an acceptable level. In particular, standards and expectations based on the components outlined in Part E of the PSM in relation to the:

  — provision of a safe and secure work environment;

  — ability to deal with emergency situations resulting from the threat of acts of violence, particularly bomb threats;

  — protection of classified information and other official resources; and

  — planning and management of conference security;
- educated staff in their responsibilities and duties within the security environment, and of the agency's security standards; and
- developed a framework for the maintenance, monitoring and review of the security environment in a timely, efficient and effective manner.

7. The ANAO also examined whether agencies had considered the risks of, and developed an appropriate policy statement on, the physical security arrangements for employees who work from home.

8. The audit scope and criteria were developed using the PSM. The ANAO also considered material gathered from research into Commonwealth public sector and international organisations' security arrangements.

9. This audit was undertaken by the ANAO to provide recommendations for improvement (where necessary), and identify and disseminate better practice observations. Accordingly, recommendations and opportunities for improvement arising from better practice observations are identified in this report. In keeping with the arrangements made for this type of audit, findings are presented generically and are not attributed to individual agencies.

10. The agencies selected for examination in this audit do not, and are not intended to, comprise a representative sample of all Commonwealth agencies. However, through this analysis the ANAO considers that other Commonwealth agencies will identify areas of opportunity in their own protective security management framework based on the lessons learnt, both positive and negative, from the agencies under examination.

Audit conclusion

Overall conclusion

11. The ANAO concluded that all agencies in the audit had made reasonable progress towards meeting their physical security responsibilities as outlined in the Commonwealth's PSM. This typically resulted in the establishment of a protective security control framework capable of limiting their exposure to, and the consequences of, their identified physical security risks.

12. Most agencies had:

- assigned and documented security responsibilities;
- obtained current National Security Threat Assessments;
- provided staff with baseline security documentation to support them in the application of security controls and procedures; and
- established arrangements to provide for a physically secure and safe work environment for their staff, contractors and clients.

13. However, the ANAO also noted a number of deficiencies across the agencies reviewed including, to varying degrees, that agencies were not:

- undertaking periodic comprehensive protective security risk assessments;
- formally considering the physical safety of staff as part of the risk assessment process;
- establishing a clear link between the risk assessment process, control selection and procedure development;
- maintaining adequate and current documentation to support the security risk, cost-benefit analysis and decision-making processes;
- applying internal controls and procedures consistently or appropriately, thereby undermining their effectiveness;
- educating their staff, contractors, and clients of agency security standards; and
- monitoring the effectiveness and cost-efficiency of the security environment and acting on identified deficiencies in a timely and well considered manner.

14. Deficiencies in the physical security segment of the protective security control framework need to be considered in conjunction with the performance of agencies in other aspects of protective security (for example, information security), as an exposure in one part of the framework may result in increased exposure on an agency-wide level.

15. This audit was undertaken at a time when Australia and its Commonwealth agencies operated in a heightened international threat environment. The events of 11 September 2001 in the United States of America initiated action by some agencies to reconsider their risk profiles and, accordingly, their security arrangements. However, recent domestic and international security events[4] have renewed the need for Commonwealth agencies to move to a more proactive protective security approach. Specifically, agencies now need to consider how to address the emerging risks of:

- international terrorism. As a result, Australian interests both here and in neighbouring countries have an increased risk profile for terrorist attacks. Recent media reports[5] also suggest that terrorist groups that are active in other countries have an increasing presence in Australia; and
- a domestic environment where threats against public officers or Commonwealth assets are probable. These events highlight that agencies need to be mindful of the ongoing appropriateness of implemented security measures, especially where Commonwealth premises: are co-located with other organisations; or may have significant negative consequences associated with a breach in their security arrangements.

16. Commonwealth agencies must acknowledge that threats and risks once thought unlikely to affect them must now be considered as possibilities. Rather than reacting to certain events, agencies should be informed as to their specific exposures, and take a strategic and thorough approach to addressing their identified risks, including relevant national security risks. To ensure the continued veracity of an agency's security environment, agencies should:

- adopt a more stringent approach to the security risk assessment, management and control. These processes should also be re-performed periodically, and in the light of any significant developments;
- develop workable and secure arrangements with co-tenants, emergency response services and other Commonwealth agencies. This is critical where:

[4] For example, the terrorist attacks in the United States of America on 11 September 2001 and in Bali on 12 October 2002, as well as the recent shooting of the Director of the Mental Health Services, Human Services Department in Adelaide on 14 October 2002.

[5] For example, *Al-Qaeda allies in Australia - ASIO*, The Sydney Morning Herald, 25 October 2002.

— agency security risks cannot be eliminated, or reduced to an acceptable level, through the implementation of internal controls;

— the nature of the event requires the guidance and direction of accredited security experts; or

— co-dependencies exist; and

- periodically remind their staff, contractors and clients of their security responsibilities.

17. These views are supported by statements issued by the Attorney-General's Department, as a result of work undertaken by the Protective Security Co-ordination Centre (PSCC). The PSCC concluded, as at June 2001, that a number of Commonwealth agencies had a weak and reactive approach to maintaining their protective security responsibilities and environments. This was typically evidenced through agencies having outdated risk assessments, inconsistent and dated security documentation, and poor quality and incomplete incident reporting.

Establishing a sound physical security environment

18. The majority of agencies effectively assigned responsibilities for physical security and information technology physical security to their senior management and security personnel. The ANAO noted that these agencies also typically recognised that it was important for them to establish lines of communication and accountability between the security personnel and the corporate management process, and that the security personnel had:

- adequate access to senior management so that their assessments and recommendations for the security environment were considered from an agency-wide perspective; and
- the authority to make (or contribute to) related decisions.

19. Most agencies had current SRAs, and the better practice agencies had established, or were in the process of establishing, enterprise risk registers to understand better, and deal with threats and risks, in the context of risk management arrangements for the whole agency. However, the ANAO considered that some agencies could be more thorough in the conduct of their SRAs, and in the analysis of the identified risks. In particular, agencies should ensure that all relevant security risks are identified and adequately considered on the basis of likelihood, consequence and risk tolerance. In addition, an ongoing environmental scan is necessary to ensure the validity of any SRA.

20. Many of the agencies need to improve their security documentation by developing and maintaining more comprehensive security plans and procedures, that are consistent, logically referenced, relevant and better tailored to agencies' requirements. Most agencies also need to improve staff and contractor education and awareness programs to ensure that security standards are applied correctly and consistently.

Components of a sound physical security environment

21. The ANAO found that all agencies in the audit had made use of a variety of protective security measures (physical, administrative, and/or personnel) to restrict access to security-classified information and other official resources. This was achieved by implementing controls and procedures designed to satisfy the majority of the minimum requirements outlined in the PSM. In addition, all agencies in the audit had made arrangements to provide their staff and clients with a safe physical work environment. However, a number of agencies were not able to demonstrate that they had approached the selection of security and safety measures in a strategic or structured manner to achieve the best results.

22. In addition, most agencies in the audit could benefit by aligning better their security, information technology (IT), corporate and emergency planning processes. While a number of agencies had sound procedures and documentation in support of their IT or emergency management arrangements, these were not adequately aligned with the other processes for maximum impact. For example, by aligning security and emergency planning processes, agencies should be able to ensure the security environment is adequately maintained in the event of an emergency situation.

23. All agencies covered by the audit had at least some security instructions that explained the controls and procedures for the protection of official information and resources. However, the quality of this documentation varied from excellent to fair. Accordingly, the ANAO recommended that a number of agencies improve their documented procedures, especially in relation to the classification, storage and handling of security-classified information and/or other official resources. In addition, many agencies also needed to develop and implement proper safeguards to control adequately the flow of classified information and official resources into, and out of, the agency.

24. It is noteworthy that all agencies in the audit made use of security guards. The degree of reliance these agencies placed on their guards varied from high to low. The ANAO observed a number of breakdowns in the application of controls by the guards, and suggests that agencies reconsider the nature and extent of their use of guards.

25. The PSM encourages a move away from security guards to electronic access control systems and intruder alarms. Regardless of the control adopted, there is always a possibility that the control may be compromised. For example, most electronic access control systems require the use of complementary controls to ensure that tailgating[6] is eliminated, and to record movements out of a secure area. However, guards may not carry out all their prescribed duties due to oversight, competing priorities or a 'decision' that a duty is not important. Therefore, agencies need to acknowledge the limitations of their implemented controls, and reduce the residual risk to an acceptable level as part of their risk management approach.

26. Agencies could also improve the cost-efficiency of their controls as the ANAO observed unnecessary redundancies in controls and procedures applied to address risks. For example, some agencies discussed staff passes in several different procedural instructions, or had implemented controls that effectively performed the same function with similar outcomes. This was typically the result of inadequate planning, documentation management and treatment analysis (for example, agencies sometimes did not identify that they had already implemented a control which contributed to the treatment of a specific security risk).

Maintaining a sound physical security environment

27. All agencies indicated that they were aware of the need to monitor and regularly review their security environments. They understood that the security environment had to change in line with internal and external threats. As a consequence, most agencies undertook some form of periodic reviews and assessments of their security threats, risks, controls and environments.

28. Despite this assurance, the ANAO found that the security personnel in almost half of the agencies approached the monitoring and review of their security environment in an ad hoc manner, and were satisfied to rely on others to manage this process on their behalf. Poor quality documentation, and competing work priorities, often meant that the security personnel of an agency were unable to capture and consider all relevant information. For example, some security incident reports did not include information on the time, location or consequences of a security event.

29. The information that was captured was generally not analysed to determine cause-and-effect relationships, nor was it used in a timely manner to update security arrangements. Few agencies established and reported against security Key Performance Indicators (KPIs). The scope of reviews did not tend to consider efficiency issues, such as the placement of equipment to best

[6] This involves an authorised or unauthorised person following an authorised pass holder through an electronically controlled access point. This action is undesirable for a number of reasons including it degrading the audit trail of access and possibly exposing classified information to unauthorised disclosure.

advantage. In a number of agencies, the security function appeared to be carried out in isolation from the other business support processes. In addition, many agencies showed that they had not considered the impact of changed work circumstances or identified threats, thereby exposing the agency to potential serious security breaches.

30. It was noteworthy that the two agencies that were subject to some form of external scrutiny from regulators maintained more detailed records and documentation in support of their security environments. This also encouraged these agencies to establish clear links between the security and agency-wide risk management functions. Therefore, it would appear that by being subject to external independent assessments, agencies may be more likely to maintain better quality documentation on their monitoring and review processes; assign responsibilities for these to staff; and internally track compliance to ensure that the external assessor is satisfied that the security environment is being maintained adequately.

Reports to agencies

31. Each of the agencies included in this audit were issued with a comprehensive management report providing conclusions against the evaluation criteria, including recommendations for improvements, where necessary. The agencies have responded to their individual findings and recommendations and have advised of remedial action being taken to address any identified deficiencies.

Recommendations

Set out below are the ANAO's recommendations with Report paragraph references. The ANAO considers that the recommendations presented below can be applied within other Commonwealth agencies when establishing, managing and improving their physical security environment. Accordingly, agencies should consider these recommendations in the context of their own risk environment, the PSM requirements and of their available resources to develop an appropriate security control framework for their requirements.

Security Risk Assessments

Recommendation No.1
Refer to paragraphs 2.45 to 2.49

The ANAO recommends that agencies conduct a comprehensive (IT, physical, personnel and information security) protective security risk assessment at least every three years as part of an agency-wide approach to risk management.

Agencies should also develop practices that assess and link the findings arising from ad hoc periodic security reviews and threat assessments, to the formal security risk assessment process undertaken every three years.

Recommendation No.2
Refer to paragraphs 2.50 to 2.52

The ANAO recommends that those officers responsible for security maintain documentation that supports their decision-making process for the prioritisation, selection and implementation of treatment options that address their identified security risks.

Security Education and Awareness

Recommendation No.3
Refer to paragraphs 2.70 to 2.75

The ANAO recommends that agencies develop and document comprehensive, consistent and logically referenced security plans and procedures.

Agencies should also develop and schedule periodic formal education and awareness programs for non-security personnel addressing agency security standards. In addition, agencies' security personnel and contractors should receive regular protective security and risk management training to ensure that they are sufficiently skilled to fulfil their responsibilities for security.

Safe Physical Work Environment

Recommendation No.4
Refer to paragraphs 3.24 to 3.27

The ANAO recommends that agencies ensure their security risk assessment process, implemented security controls, and documented security procedures, adequately address all staff safety concerns as discussed in Section 5 of Part E of the PSM.

Protection of Security Classified Information

Recommendation No.5
Refer to paragraphs 3.71 to 3.74

The ANAO recommends that agencies ensure their security risk assessments, implemented security controls, and documented security procedures adequately address all requirements for the storage, handling and processing of any security-classified information as discussed in Section 7 of Part E of the PSM.

Security Monitoring and Review

Recommendation No.6
Refer to paragraphs 4.38 to 4.41

The ANAO recommends that agencies improve the procedures surrounding the reporting and recording of physical security incidents to ensure that all relevant information is captured in a timely manner, and used constructively to improve the security environment.

Audit Findings and Conclusions

1. Introduction

This chapter of the report provides an overview of the Commonwealth's Protective Security Policy framework and objectives. It describes the components of the framework, and explains its importance in managing security risks that impact on the Commonwealth's information, assets, personnel and clients. It highlights the role that physical security measures have in protective security, and discusses contemporary physical security issues to illustrate the risks and consequences of inadequate physical security measures.

Commonwealth Protective Security Policy

1.1 Each Commonwealth agency[7] has an obligation to create and maintain an appropriate protective security environment for the protection of its functions and official resources.[8] The Commonwealth's protective security policy framework exists to assist Commonwealth agencies with the identification and design of controls and procedures that will protect their official information, assets and human resources from potential security threats and risks.

1.2 Guidance is provided to agencies in the Commonwealth Protective Security Manual (PSM). Responsibility for the development of this manual rests with the Commonwealth Attorney-General. The Attorney-General is supported in this role by the Protective Security Coordination Centre (PSCC), which promotes, educates and provide input to, and feedback on, the status of protective security within the Commonwealth. This advice is used to assist with the periodic revision and improvement of the PSM. The most recent edition of the PSM received endorsement by the Government in September 2000.

1.3 The Government has, on several occasions, emphasised the importance it attaches to protective security, particularly highlighting the importance of maintaining an effective level of security awareness. The current PSM proposes a risk-based control framework for protective security management within

[7] The PSM defines the term 'agency' to include all Commonwealth Government departments, authorities, agencies, or other bodies established in relation to public purposes, including departments and authorities staffed under the *Public Service Act 1999*.

[8] op cit, A5, Section 1.4.

Commonwealth agencies. The control framework comprises a number of complementary measures including:

- physical security measures (for example, perimeter and building access controls);
- administrative security measures (for example, the classification of official information); and
- personnel security measures (for example, the assessment of the honesty and integrity of personnel).

1.4 To establish an effective and efficient protective security control framework within an agency, these complementary measures need to be considered in light of the agency's contextual, internal and external risks. Identified risks should be addressed through appropriately designed controls and procedures, which are applied diligently and consistently.

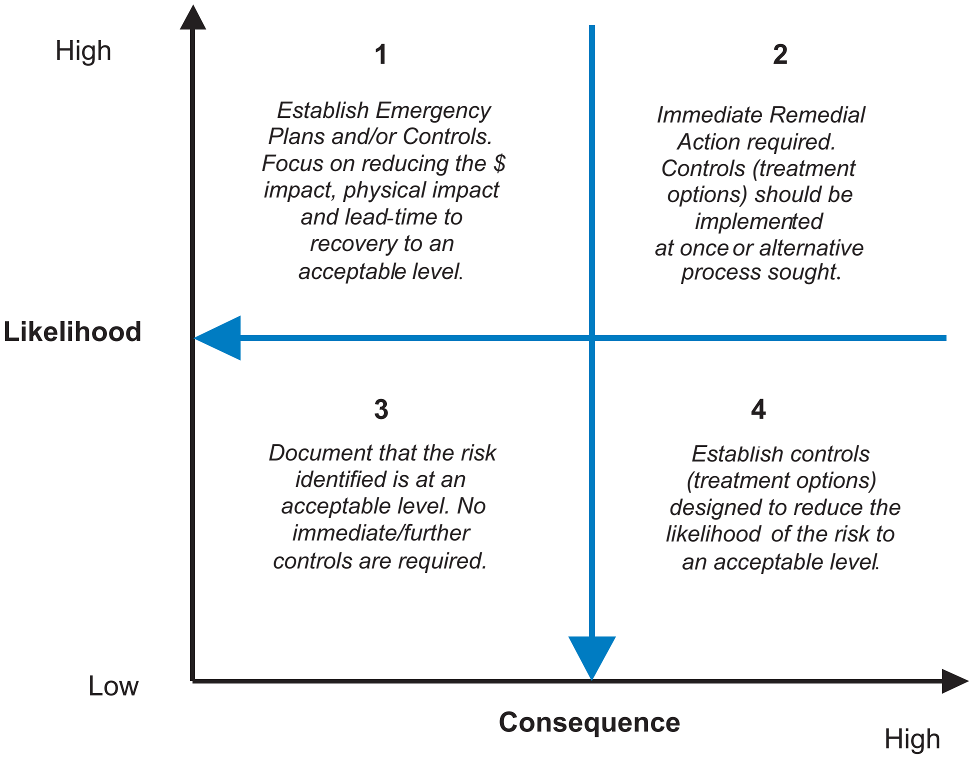
Physical security measures

1.5 Physical security is an essential element of the protective security framework. Part E of the PSM outlines the Commonwealth's policy framework for physical security measures, as well as the recommended procedures and minimum standards. It also discusses agencies' obligations under other relevant related legislation, including the *Occupational Health and Safety (Commonwealth Employment) Act 1991*, as they apply in a physical security context. Specifically, Part E of the PSM is concerned with controls and procedures that are designed to ensure an agency has a safe and secure physical environment for the protection of the Commonwealth's information, assets, personnel and clients.

1.6 These controls and procedures should be capable of deterring and detecting attempted breaches to the agency's protective security environment, and should also provide agency security personnel with the information they require to assess and communicate the necessary actions to prevent a crime, or minimise its consequences. In addressing their protective security risks, it is necessary for agencies to understand that controls and procedures typically either reduce the consequence of a risk, or the likelihood of the risk eventuating. The overall objective for the agency is to implement a series of mechanisms that will reduce the agency's risk to an acceptable level. These principles are illustrated in Figure 1.

Figure 1

Risk Management Decision Matrix


High
Likelihood
Low
Consequence
High
1
Establish Emergency Plans and/or Controls. Focus on reducing the $ impact, physical impact and lead-time to recovery to an acceptable level.
2
Immediate Remedial Action required. Controls (treatment options) should be implemented at once or alternative process sought.
3
Document that the risk identified is at an acceptable level. No immediate/further controls are required.
4
Establish controls (treatment options) designed to reduce the likelihood of the risk to an acceptable level.

1.7 Figure 1 illustrates the relationship between likelihood and consequence, and how this is related to the implementation of appropriate controls designed to reduce security risks to an acceptable level. For example, a risk that has a high likelihood of eventuating, but a low consequence in terms of the loss or harm to official resources, would be located in Quadrant 1. Similarly, Quadrant 4 covers risks that are unlikely to eventuate, but if they did, they would result in significant loss or harm to official resources.

1.8 The allocation of risk ratings based on the location of the risk in the decision matrix will enable the prioritisation of acceptable and unacceptable risks. Agencies should work to isolate risks to the bottom left portion of the matrix (Quadrant 3), but are likely to tolerate risks in Quadrant 1 due to their relatively low consequence (as illustrated by the blue arrows dissecting the matrix).

1.9 Agencies must also be mindful that they are required to develop solutions within limited timeframes and with restricted resources. Agencies therefore need to apply their scarce resources in a timely manner to generate the most efficient and effective security control framework possible.

Impact of poor physical security measures

1.10 Poor physical security controls and procedures expose an agency to unnecessary risks. The realisation of these risks may include injured or distressed staff or clients, stolen property or compromised information, or worse, result in an event that impacts adversely on national security.

1.11 It is important for agencies to understand that an exposure in one element of its security environment is capable of undermining the total protective security framework. Therefore, the security framework will be more robust if the physical measures are complemented by administrative and personnel security measures. These principles are more fully explored in other parts of the PSM, but are referenced within Part E. The linking of these principles is necessary as, ultimately, any protective security control framework is concerned with limiting the potential for the integrity, availability and confidentiality of official information, assets, personnel and clients to be compromised or harmed. It is possible that physical controls and procedures may not be the most effective and cost-efficient mechanism for this purpose. Rather, an integrated framework of administrative, personnel and physical controls and procedures should be used to address the total protective security framework in a more effective and cost-efficient manner. An agency which adopts this approach is acknowledged as having security-in-depth[9] (this principle is explained in Chapter 3).

Applying the Commonwealth Protective Security Policy

Developing a control framework and assigning responsibilities

1.12 Within each Commonwealth agency, the agency head typically assigns the responsibility for the establishment and oversight of the security environment to the security executive. The security executive then delegates the responsibility for implementing and ensuring compliance with the agency's protective security policy and procedures to the Agency Security Adviser (ASA) and the Information Technology Security Adviser (ITSA).

Understanding and managing security risks

1.13 In order to establish an appropriate protective security environment, an agency will need to complete a Security Risk Assessment (as outlined in Part B, *Guidelines on Managing Security Risk* of the PSM) to determine its risk profile. The security personnel should prioritise the identified risks and develop a series of possible treatment options. It is important to recognise that risks may be internally or externally sourced, with internal risks being more difficult to control

[9] Refer to paragraph 2.4 of Part E of the PSM, p. E7.

due to an inherent level of trust necessary to complete agency functions. Nevertheless, the agency must address all its risks under its duty of care to the Commonwealth. It is also important to understand the context of the risk in order to design the most effective control to prevent its occurrence or limit its impact.

1.14 Based on a detailed consideration of the protective security threats and risks, resource value,[10] classification of information and site characteristics, the security executive (or governing body) should oversight the selection, development, and implementation of controls and procedures that create an appropriate security environment. To ensure the requirements of this environment are understood and adhered to, the agency should document its chosen controls and procedures in an Agency Security Plan (ASP), and develop education and awareness programs to communicate these principles to its personnel. More specifically, the physical security controls and procedures should be documented in a Site Security Plan (SSP), for use by the security personnel in administering the security environment.

Maintaining the security environment

1.15 An agency should monitor and continue to re-assess its risks and security environment once established, to ensure that its security arrangements remain adequate.

External assistance

1.16 There are a number of organisations available to assist in assessing and establishing an appropriate protective security environment. These organisations include the:

- Australian Security Intelligence Organisation (ASIO) and the PSCC, for advice on threat and risk assessments;
- Australian Protective Service (APS) and ASIO's T4, for advice on physical security measures and risk assessments; and
- Security Construction and Equipment Committee (SCEC), for advice on, and evaluation of, security hardware, equipment and systems.[11]

[10] Refers to the intrinsic value of the resource to the agency. This may be a factor of the financial value, or a factor of the degree to which the resource contributes to the overall outputs and outcomes of the agency.

[11] Agencies also have access to the Security Equipment Catalogue (SEC) to assist with the selection of security equipment. This catalogue was recently revised. ASIO's Annual Report to Parliament for 1999–2000 reported that the SEC was revised in 1999–2000 to reflect updated standards for security equipment. It also reported that staff shortages and the refurbishment of the Canberra test site had restricted ASIO's ability to test and evaluate a number of security devices in use, creating a backlog in testing.

Contemporary Physical Security Issues

1.17 The introduction of changed work practices, such as an increasing reliance on information technology, outsourcing and home-based work practices, together with a changing national and international security risk environment, has resulted in an increased need for the Commonwealth and its agencies to reconsider their vulnerabilities and risks. Emerging risks and vulnerabilities have to be identified by agencies, understood, and managed to prevent the occurrence, or minimise the impact, of harm.

1.18 Current reviews and studies have considered the status and impact these issues have had on the protective security framework. Further reviews of protective security policy and practices will strengthen the impact of the PSM based on the lessons learnt from agencies' adaptation of the minimum standards.

1.19 It is worth noting that some of the recently reported physical security breaches in Australia have been designed more to draw publicity and media attention without actually compromising the resources under protection.[12] In addition, international terrorist events may raise the threat profile of Commonwealth agencies. However, agencies may assess that such threats have a low likelihood of occurrence. Therefore, it is important for agencies to distinguish between high-visibility, low-likelihood risks, and other risks which are more likely to impact the agency in the immediate term, and develop appropriate responses based on the assessment of the likelihood and consequence of the risks. The focus is on sound risk management.

Report on the results of the Commonwealth Protective Security Survey of 2001

1.20 On 14 September 2000, the Government decided that the Protective Security Policy Committee (PSPC) should report annually on the status of protective security within Commonwealth agencies.[13] For the year ended 30 June 2001, Commonwealth agencies were requested to participate by completing an 86-question survey. This survey was designed to collect data for analysis of the extent of compliance with the minimum protective security standards prescribed in the PSM.

[12] For example, Greenpeace incursions at the Lucas Heights Science and Technology Centre on 17 December 2001 and the Australian Parliament House on 19 August 2002.

[13] The requirement for the PSPC to report annually to SCNS was one of the general recommendations arising from the Inspector-General of Intelligence and Security inquiry of 1999 on measures to be taken to strengthen the protection of classified information against espionage.

1.21 The first annual report on the status of protective security in Commonwealth agencies as at 30 June 2001 was delivered to government in June 2002. The findings indicated that awareness of protective security policy across Commonwealth agencies needed to improve, and that the development and maintenance of Agency Security Plans (ASP) was a critical first step in generating a positive security culture.

1.22 Overall, the report identified that the status of physical security was generally sound. However, deficiencies were noted in the agencies' application of the complementary measures of personnel security and/or information security. Complacency was identified as an issue in some agencies. In others, there was a lack of commitment to structured processes and practices. In addition, there was generally a low level of understanding of the minimum standards of the PSM.

1.23 The last PSA published by the ANAO, titled *Personnel Security—Management of Security Clearances*,[14] highlighted that there were a number of deficiencies in the management of the risk assessment and vetting processes. These could potentially undermine soundly planned and managed physical security arrangements by permitting inappropriate people access to classified information and resources.

1.24 The PSPC is currently undertaking the second year of its review of the status of protective security in Commonwealth agencies. Agency responses were due on 30 October 2002.

1.25 The PSPC also has a program in place to review selected components of the PSM each year. At the time of the audit, reviews of Part D (Personnel Security), Part B (Risk Management) and Part G (Investigations) were in progress. Parts C (Information Security) and E (Physical Security) are scheduled for review from 2003.

The events of 11 September 2001 and 12 October 2002

1.26 In accordance with the National Anti-Terrorist Plan, and the associated uncertainty of the international environment, Australia was placed on a heightened security alert following the terrorist attacks on the United States of America (USA) on 11 September 2001. A news release on Australia's National Security from the Attorney-General dated 18 September 2001, acknowledged that the attacks on the USA had fundamentally changed the global environment in which we live and the impact of these will reverberate for years to come. The recent events of 12 October 2002 in Bali are still being evaluated but will also have an impact.

[14] Refer to ANAO Audit Report No.22 of 2001–2002.

1.27 The general threat environment has also changed, inferring a need for more timely and thorough assessments of security threats and risks that may impact on an agency's physical security environment. This climate has also reminded agencies that they not only have to protect classified information, they also have to protect their assets, personnel and clients.

1.28 The ANAO acknowledges that issues such as those mentioned above are dealt with more thoroughly by agencies in the disciplines of emergency and business continuity planning. Protective security concerns itself primarily with known (measurable and likely) and recurring security threats and risks. However, the agency's protective security policies, plans and procedures should be integrated with the documents prepared under these other disciplines to form an integrated control framework that can withstand both common, and unlikely, security events.

Report structure

1.29 This report outlines the audit findings by categorising protective security concepts and principles in the subsequent chapters as follows:

- Chapter 2 of this report discusses the key components and steps that are critical to establishing a sound physical security environment;
- Chapter 3 of this report discusses the core components of the physical security environment as prescribed in the Commonwealth's protective security policy; and
- Chapter 4 of this report outlines the components of a successful monitoring, maintenance and review cycle for the physical security environment.

1.30 A summary of the sound and better practice observations is provided at the conclusion of each chapter.

2. Establishing a Sound Physical Security Environment

This chapter outlines the key components and steps which are critical to the establishment of a sound protective (and in particular, physical) security environment within a Commonwealth agency. The chapter explains that physical security is one component of the total protective security control framework, and explains the relationship between physical security and the other components. The importance of the protective security risk assessment process is examined, as well as the security management oversight function. Recommendations and opportunities for improvement identified in the agencies audited are discussed. In addition, a summary of the sound and better practice observations made during the audit is provided at the conclusion of the chapter.

Introduction

2.1 A robust protective security control framework[15] is a critical component of an agency's total governance framework. It directly influences the success and effectiveness of any policies developed for that agency's security environment, as well as the controls implemented to support it.

2.2 A structured and informed protective security control framework contains many components, including clearly defined objectives, lines of accountability, delineation of responsibilities, and adequate supporting processes and procedures. Within this framework, agencies also need to plan and budget for their security environment, as well as undertake risk assessments, performance measurement and assessment, and management reporting. The security executive should be assigned the responsibility for oversight of the implementation and management of the security environment in an agency. In addition to these components, senior management endorsement of documented policies and decisions will greatly assist in the acceptance of standards for security throughout an agency.

2.3 As noted earlier, the physical security environment is one component of the total protective security framework. This audit specifically examined the approach to developing, implementing and maintaining adequate physical security environments in seven Commonwealth agencies.

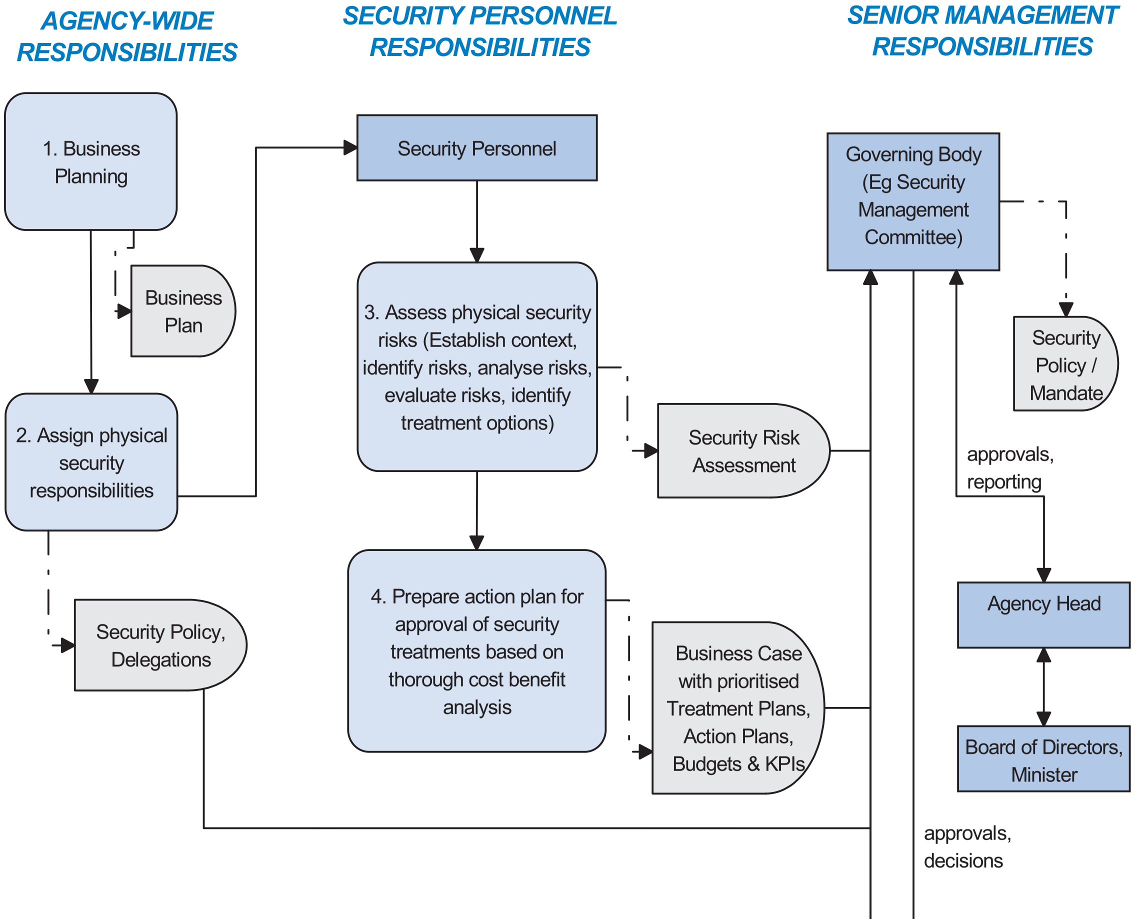
Application of Commonwealth Guidance by agencies

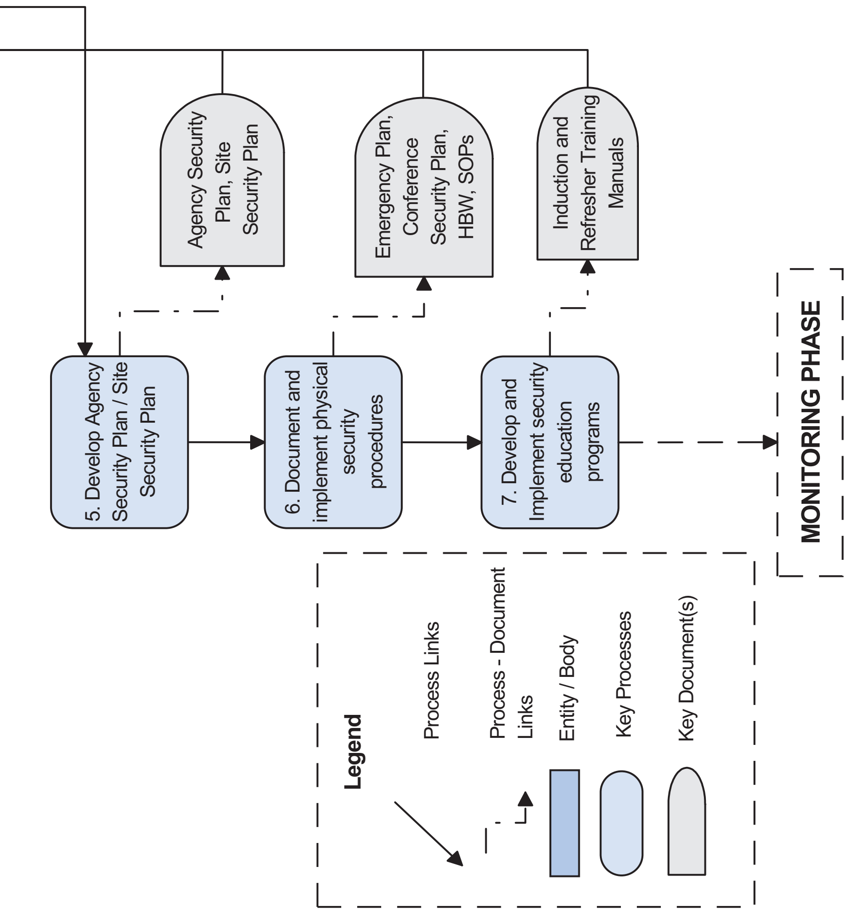
2.4 Figure 2 illustrates the critical processes in the total protective security control framework that are relevant in establishing a sound physical security environment. These processes are explained in further detail in the following section.

[15] The control framework provides an important link between the organisation's objectives and the functions and tasks undertaken to achieve those objectives. For more detail on the components of a control framework, refer to the ANAO's better practice guide titled, *Controlling Performance and Outcomes*. Available from <http://www.anao.gov.au>.

Figure 2

Establishment Phase of the Physical Security Control Framework


AGENCY-WIDE RESPONSIBILITIES
SECURITY PERSONNEL RESPONSIBILITIES
SENIOR MANAGEMENT RESPONSIBILITIES
1. Business Planning
Business Plan
2. Assign physical security responsibilities
Security Policy, Delegations
Security Personnel
3. Assess physical security risks (Establish context, identify risks, analyse risks, evaluate risks, identify treatment options)
Security Risk Assessment
4. Prepare action plan for approval of security treatments based on thorough cost benefit analysis
Business Case with prioritised Treatment Plans, Action Plans, Budgets & KPIs
Governing Body (Eg Security Management Committee)
Security Policy / Mandate
approvals, reporting
Agency Head
Board of Directors, Minister
approvals, decisions


Agency Security Plan, Site Security Plan
Emergency Plan, Conference Security Plan, HBW, SOPs
Induction and Refresher Training Manuals
5. Develop Agency Security Plan / Site Security Plan
6. Document and implement physical security procedures
7. Develop and Implement security education programs
MONITORING PHASE
Legend
Process Links
Process - Document Links
Entity / Body
Key Processes
Key Document(s)

Establishing a sound physical security environment

2.5 Prudent management of the physical security environment is needed to achieve the most appropriate and cost-effective combination of procedural and physical measures, and reduce security risk to an acceptable level.

2.6 Initially, agencies will need to establish a control framework for security management and assign responsibilities. This may include the formation of a governing body (for instance, a security management committee) to undertake the planning, management and oversight of the security environment, or these duties may be assigned to an existing body such as the agency Audit Committee. The governing body will need to be supported by a mandate and its function should be communicated in a policy statement together with the agency's philosophy and stance on security. It is critical for employee buy-in and support to be sought from all areas of the agency (and where relevant, other stakeholders[16]) to establish an effective agency-wide approach to security issues.

2.7 The governing body should determine the agency's security risk environment through the conduct of a SRA. This will assist it to make decisions about creating an appropriate physical security environment that is based on relevant and complete information. Sound and efficient analysis and decision-making practices are also required.

2.8 To be fully effective, staff, contractors and clients should be aware of the agency's security requirements. Therefore, the agency must develop and maintain adequate supporting documentation and education programs (based on the agency's requirements), which clearly communicate the security responsibilities, requirements, expectations and decisions. This will include the development of an ASP and Site Security Plan (SSP).

Audit findings—Establishing a Sound Physical Security Environment

2.9 This section provides some contextual information on each of the key components the ANAO examined when considering agencies' security control frameworks. A discussion of the findings in the seven agencies audited is then provided to highlight:

- examples of sound and better practices; and
- opportunities for improvement.

[16] For instance, industry regulators and other building occupants where there are shared premises.

Assignment of roles and responsibilities

2.10 Each agency should establish an appropriate framework of responsibilities and accountabilities for security management.

2.11 As mentioned previously, the agency head will typically assign security management responsibility to one of the agency's Senior Executive Officers (SES), who will act as the security executive for that agency. This position would oversee the development and management of protective security matters within the agency. The security executive may achieve this through chairing or participating in a governing body for security, and appointing an ASA and ITSA.

2.12 The ASA and ITSA should be responsible for ensuring that the agency's security policies standards are implemented and adhered to. They provide ongoing (daily) support and advice to the line managers and agency staff, and should be capable of assisting in the strategic and operational planning arenas (although this is typically only the case in better practice agencies).

2.13 ASAs and ITSAs perform a number of duties as part of their role. These include, but are not limited to:

- participating in the risk assessment process;
- preparing and monitoring a security budget;
- assisting with the development of security policies and other documents;
- managing outsourced security contracts;
- ensuring adherence to the implemented security standards;
- educating staff on agency security practices; and
- providing feedback to management on the effectiveness and cost-efficiency of the adopted mechanisms and procedures.

2.14 The ASA and ITSA can engage security consultants[17] to assist them in undertaking any of these activities. Indeed, the PSM requires some assistance to be sought in certain circumstances.[18] For instance, if the level of classified information held by the agency is SECRET or above, a National Security Threat Assessment (NSTA) must be sought from ASIO.

[17] Refer to the suggested list of organisations listed from paragraphs 6.30 to 6.37 of Part E of the PSM, pp. E33 and E34.

[18] Refer to the ready reckoner on p. E42 of the PSM.

2.15 The ASA and ITSA need to have sufficient access to management to be effective administrators of the security management process. This may be achieved by making these officers part of the governing body for security and/or by appointing them to a sufficiently senior position within the agency that has the necessary authority.

Agency findings

2.16 All agencies in the audit had appointed an SES officer as the security executive equivalent, and were reporting on security management matters to a governing body. Three agencies had a separate security management committee. The other four agencies reported security matters directly to a corporate management board. All but one agency had clearly established the security function's mandate in its corporate documentation.

2.17 All agencies had appointed an ASA. This person had appropriate access to senior management to enable them to make a contribution to the security decision-making process. In four agencies the ASA was able to make a contribution through (but not as) a member of the governing body. However, in two of these agencies, there were several levels of management between the ASA and senior management. In the remaining three agencies, the ASAs were part of the governing body.

2.18 The ANAO notes that, even though an absence of direct liaison between the ASA, and the governing body or senior management could have been expected to have a negative effect on security management, this was not generally observed. The ANAO found that the level of the ASAs had more impact on the degree of their contribution, than on their membership of the governing body. This confirms that ASAs need to have a sufficiently high profile to enable them to perform their role effectively.

2.19 The ANAO noted that the majority of ASAs which were solely dedicated to security activities were not on their agency's governing body for security. The ASAs who were members of their agency's governing body for security also performed other administrative roles within their agency (for example, building maintenance).

2.20 Most agencies had delegated the ITSA role to the Information Technology (IT) Manager. While these officers were best qualified to perform the assigned task, there were only three agencies that actively involved (and showed any evidence of) the ITSA in the security management process. In the other four agencies, the ITSA operated in a relatively isolated manner. However, the ANAO found that this did not adversely affect the security environment. This was due to the agencies taking a thorough approach to IT security management and implementing sufficient controls to protect the physical security of the equipment and information. Nevertheless, this finding did not mean that these agencies had not missed opportunities for economies of scale in the design and selection of their controls and procedures. The ANAO considers that other Commonwealth agencies may find that they cannot achieve total protective security coverage, or obtain the best strategic advantage from the security function, by operating in this manner.

2.21 The ANAO found that three agencies had developed detailed documentation on the delineation of responsibilities for security within their agency, and had directly linked this to the corporate delegations of authority. Another agency had summarised, at a high level, in its policy statement, its security responsibilities and had prepared a matrix of responsibilities by line area and risk item. However, this had not been linked to the corporate delegations. In the remaining three agencies, responsibilities for security between the ASA, line areas and contractors had been defined and documented, but these were out-dated due to agency restructures. These three agencies are currently in the process of reviewing relevant responsibilities.

2.22 The ANAO also noted that four agencies showed inconsistencies between responsibility descriptions and position titles across their agency's various security documents. This has lead to some confusion over accountabilities and, consequently, creates a risk for these agencies.

2.23 Four agencies had included a paragraph in their key security policy document stating that all staff were active participants in upholding the security standards of the agency. Another two agencies had documented this requirement, but could strengthen the association by documenting this requirement in their policies, rather than in their lower level procedures. Only one agency had not explicitly communicated to its non-security staff their responsibility for ensuring that sound physical security procedures are upheld throughout the agency.

2.24 The ANAO also noted that six agencies require their staff to sign a security or confidentiality declaration form on commencement, acknowledging their responsibility in relation to agency security or confidentiality.

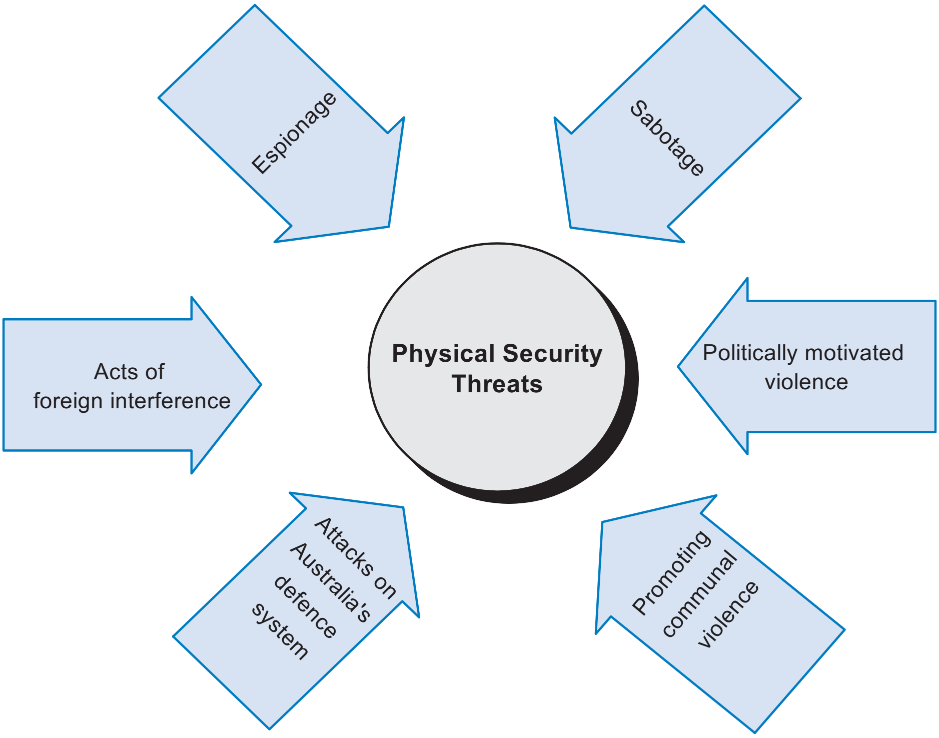
Security risk management

2.25 As mentioned in Chapter 1, agencies are required by the Commonwealth to undertake an appropriate and thorough security risk management process. The objective of the security risk management process is for the agency to establish a security environment that provides adequate protection for its functions and responsibilities. This includes ensuring the delivery of its business outcomes, and the protection of the public's confidence in the safety of the:

- agency;
- official resources owned or held by the agency; and
- staff and clients of the agency.

2.26 The two primary types of risk that the agency needs to address for the purpose of Part E of the PSM are: physical or other harm to people; and the misuse or compromise of official resources, particularly information. There are a number of other threats and risks that the agency needs to consider as part of the SRA process. Threats and risks may arise from sources within and/or outside the agency, and take various forms as indicated in the following diagram.[19]

Figure 3
Physical Security Threats and Exposures


Espionage
Sabotage
Acts of foreign interference
Physical Security Threats
Politically motivated violence
Attacks on Australia's defence system
Promoting communal violence

2.27 For example, the source may be disgruntled staff and they may undertake or facilitate an action of sabotage. The motivation behind the threat, and ability to access classified information and other official resources, are quite different depending on the source. Therefore, the agency needs to give due consideration to the variety of threat and risk combinations that it may face, based on its own agency context, and develop treatment options accordingly.

[19] Part B of the PSM provides a more comprehensive listing of the source, motive and method of operation of threats.

2.28 ASAs are provided with guidance on the recommended approach to this process in Part B of the PSM. Agencies can also engage security consultants, and utilise their security-based tools, to assist with this process.

2.29 Part B of the PSM recommends that agencies adopt a risk management methodology consistent with the principles of general risk analysis and management as outlined in the Australian / New Zealand Standard on Risk Management (AS/NZS4360:1999).[20] This methodology, as adopted within the PSM, involves agencies undertaking a structured and considered process to assess and deal with the security risk environment. It requires each agency to:

- establish the agency context;
- identify, analyse and evaluate the security risks;
- treat the security risks (and prepare a security plan); and
- implement an effective monitoring and review mechanism (which is discussed in more detail in Chapter 4).

2.30 Table 1 summarises the key risk management principles that agencies should consider when determining or reviewing their security risk environment.

2.31 The first, fourth and seventh principles highlight that, in order for an agency to make an informed decision about its protective security control framework, the agency should first identify agency-wide risks and objectives,[21] and determine the most cost-efficient and effective use of its available resources across all of the agency's functions and roles. Typically, this analysis involves a consideration of the likelihood of the risk materialising, together with the:

- cost (financial and operational efficiency) to the agency of the proposed treatments and their residual risks; and
- consequence to the agency if the treatment is not selected.

2.32 The security risk management process will only be effective if it is completed prior to the development or revision of the security standards and procedures.

2.33 The agency must keep in mind that this decision process must be robust and supportable, as a failure to implement protective procedures, when the risk review indicates they are necessary, would expose the Commonwealth to an unacceptable risk. It may also have implications for information sharing and consultative arrangements between agencies that are essential to the efficient operation of government.[22]

[20] Refer to paragraph 1.5 of Part B of the PSM, p. B5.

[21] Also refer to discussion in paragraph 4.1 of Part E of the PSM, where it is highlighted that an appropriate physical environment cannot be established until a security risk review has been completed.

[22] Refer to paragraph 4.15 of Part E of the PSM, p. E15.

2.34 Equally important, is the need for security decisions to be made on the basis of current, relevant and complete information. The PSCC states in its training material that the government expects agencies to review their security plans, and risk status, annually. The frequency of the risk review process directly affects the quality of the security environment, as in the absence of a current risk assessment it is difficult, if not impossible, to objectively identify and address security risk exposures. This matter is also discussed in Chapter 4.

Table 1

Risk Management Principles[23]

1	**Good security risk management is based on a clear and concise understanding of the aims, functions and goals of the agency.** *These should be clearly referenced in the security policy.*
2	**Agencies need to apply a systematic and coordinated approach to develop and establish a program for managing security risks.**
3	**Developing and establishing a program for managing security risks also requires consideration of legislative and policy standards.** *Agencies should document these as minimum standards in the security plan.*
4	**Planning against security risks should become part of an agency's culture. It should be integrated into the agency's philosophy, practices and strategic and operational plans, not viewed or practised as a separate program.**
5	**Security reviews, audits and plans should be based on comprehensive, current and reliable information.**
6	**Security risk planning and treatments need to be focused on where there is a significant risk.** *Therefore, security planning must involve a careful analysis of the risks to decide whether the risks warrant treatment. To do this, there should be a thorough assessment of the consequences and the likelihood of the risk.*
7	**Security plans should concentrate on providing treatments which are appropriate to the level of risk and are cost-effective.** *Risks need to be assessed against corporate goals, and treatments prioritised. Proposed treatments should be subject to a cost-benefit analysis.*
8	**The security treatments and the agency's operating environment should be monitored and assessed regularly.** *As well as an evaluation of the effectiveness of current security treatments, the implications of changes to an agency's functions, responsibilities and risk profile will need to be considered. Security incidents will also need to be investigated, and their impact on the security plan assessed.*

[23] Refer to Part B: Guidelines on Managing Security Risk, of the PSM.

Agency findings

2.35 Only one agency did not have a current Protective Security Risk Review (PSRR) or NTSA. However, it indicated that it had sought ad hoc advice on security risks from ASIO, as well as undertaking thorough business and fraud risk assessment processes.

2.36 The ANAO cautions that business and fraud risk assessments may complement, but are not substitutes for, a PSRR/SRA as the purpose of these reviews can be quite different. For instance, fraud risk assessments may consider the risk of a misappropriation of funds from accounting systems, and therefore focus primarily on system and accounting controls, whereas a protective security risk assessment will focus on all matters pertinent to the physical protection of agency resources and staff.

2.37 Four agencies had established, or were establishing, a register of risks in order to monitor the changing threats and risks to their agency. Two of these agencies had already linked the risk register to the overall risk management framework. Another of these agencies planned to implement software to assist with the management of the register, and had plans to incorporate this into the overall risk management framework of the agency.

2.38 The ANAO found evidence that four agencies had completed their SRAs in a manner consistent with the principles of the risk management standard AS/NZS4360. A further two agencies evidenced that they had also linked the security risk and agency-wide risk assessment processes to form a robust, iterative and integrated framework. Of the agencies that had a current (in the last three years) PSRR, all contained some discussion of physical security risks. In addition, these agencies had identified in their SRAs the likelihood and consequences of risks. However, few evidenced that they used this analysis to focus their management efforts on dealing with such risks.

2.39 There was little detailed discussion in agencies' SRAs of the risks when one Commonwealth agency shares information with another Commonwealth agency. Given that this is one of the minimum standard requirements specified in Part E of the PSM, the ANAO considers that this is an area where risk assessments could improve across the Commonwealth. The ANAO notes that the Commonwealth Protective Security Survey of 2001 confirmed this was an issue for agencies in 2001.

2.40 Some agencies also had only limited evidence that the security of their systems and electronic information was adequately linked to the other security or risk assessment processes. Most agencies that processed security-classified information on their IT systems indicated they had consulted the Defence Signals Directorate (DSD) or considered Handbook 14 of the Australian

Communications-Electronic Security Instruction (ACSI) 33. The detailed IT risk assessments were generally conducted separately from the SRAs, and contained only a high-level discussion of IT security risks. In addition, most agencies did not maintain adequate documentation to evidence their work, correspondence or reference to standards for IT security.

2.41 The ANAO noted that four agencies did not maintain adequate documentation on their SRAs, treatment plans and decisions on cost-benefit analysis (for example, evaluation of treatment options on the basis of likelihood and consequence). In essence, there was no available evidence as to whether they had undertaken this process appropriately. There was also a lack of evidence in these agencies to suggest that there was senior management endorsement of the chosen course of action. The lack of documentation made it difficult to establish any links between the policies, standards and expectations established, and the risk assessment process.

2.42 The ANAO found that, in four agencies, the timeframe taken to respond to the findings of risk reviews meant that circumstances had changed that were likely to affect the desired course of action. However, only one of those agencies could provide evidence that it had reviewed a previous decision in light of new information. Poor quality or incomplete documentation also meant that there was little opportunity for economies of scale or sound decision-making when reconsidering risks in the future or under changed circumstances.

2.43 All agencies indicated that some records of physical security costs were maintained, and that these were generally part of the corporate budget. However, cost information on security was not readily available in some agencies. It was apparent that not all costs are recorded. Further, it did not appear that this information (or incident reports for some agencies) was used to assess the cost efficiency or effectiveness of the treatment adopted.

2.44 All agencies indicated that they sought the assistance and advice of security experts, such as ASIO, when selecting security products and undertaking risk assessments. In addition, all agencies indicated that they referred to the SCEC catalogue when selecting treatments and products. However, the ANAO found that two agencies were not able to provide evidence that they had used this advice in the decision-making process. This increases the likelihood that these agencies may select non-endorsed security products, or have maintenance performed that compromises the integrity of the mechanism.

Recommendation No.1

2.45 The ANAO recommends that agencies conduct a comprehensive (IT, physical, personnel and information security) protective security risk assessment at least every three years as part of an agency-wide approach to risk management.

2.46 Agencies should also develop practices that assess and link the findings arising from ad hoc periodic security reviews and threat assessments, to the formal security risk assessment process undertaken every three years.

2.47 As a part of any future security risk review, agencies should ensure that they apply a risk assessment process that is consistent with that outlined in Part B of the PSM, and that all risks identified are documented and considered through the development of a risk register and treatment option plan. Ideally, the risk assessment process will precede the implementation of controls and development of procedures.

2.48 When identifying possible threats and risks, agencies should refer to guidance and seek the assistance of security professionals to ensure that they address all relevant security risks. In addition, under a decentralised operating environment, or a shared security management scenario, agencies need to be careful that all parties actively participate in, and contribute to, the information gathering and decision-making process. If this is not occurring, the governing body or security executive are likely to be making decisions on the basis of incomplete or biased information.

2.49 Agencies would benefit from developing enterprise-wide and business unit level risk registers. These risk registers should also document security risks. Agencies then need to establish a link between these registers, and their security expectations and documentation. Changes to the risk environment need to be analysed and taken up in a timely manner to ensure the ongoing effectiveness of the security environment.

Recommendation No.2

2.50 The ANAO recommends that those officers responsible for security maintain documentation that supports their decision-making process for the prioritisation, selection and implementation of treatment options that address their identified security risks.

2.51 As part of this approach, agencies should conduct, and maintain evidence of, the cost-benefit analysis that evidences their consideration of the likelihood and consequence of the identified risk. The chosen treatment options should be prioritised in an action plan based on an assessment of risk tolerance. This plan should also highlight responsibilities and timeframes for the implementation of actions, and identify any key deliverables. These documents should support the agency’s approach and decisions in relation to its security environment.

2.52 The sentiments of these recommendations, and the principles outlined in the discussion above, were recently reflected by the House of Representatives Standing Committee on Legal and Constitutional Affairs, where the Committee recommended that ***all agencies adopt a comprehensive security system such as that provided by the Protective Security Manual. Agencies should adapt the general standards to their particular circumstances.***[24] This recommendation also highlighted that the PSCC and DSD are available to assist agencies with adapting the standards.

Documentation of policies, standards and expectations

2.53 An agency must document a security policy, plan and set of procedures to ensure that a common understanding of the security standards is achieved.

2.54 The security policy will be the overarching document that explains, at a high level, the agency's philosophy towards security and its expectations of its staff.

2.55 The ASP should communicate the system of controls and barriers designed to deter any potential intruder from accessing or causing harm to official information, assets, personnel or clients. It should include a discussion of all of the protective security measures (physical, personnel, logical and procedural) as they apply to the agency. It should also be possible to link the system of controls and barriers to an agency's risk assessment and security framework decisions. This document should be supplemented by a SSP (to be used by security personnel) that outlines the site details, protective security measures and operational requirements.

2.56 The security procedures should provide management and staff with the necessary guidance to implement the agency's security standards. Their nature and content will vary between agencies. Their purpose is to convey the practical information on 'how to' and 'in what circumstances' to deal with identified issues. Security procedures generally cover matters such as the classification, storage and handling of classified information, information technology security requirements (for example password maintenance), the need-to-know principle, the clear desk policy, and the management of keys and combinations. Examples of these procedures, and the associated mechanisms and controls used to enforce them, are discussed in more detail in Chapter 3 of this report.

[24] Refer to Recommendation 11 of the *'In-Confidence': The House of Representatives Standing Committee on Legal and Constitutional Affairs Report of its inquiry into the protection of confidential personal and commercial information held by the Commonwealth*, 20 August 2002, p. 5 [DHOR 2002].

Agency findings

2.57 All agencies in the audit had developed some security documentation, which was generally made available to staff on agency intranets. Two agencies had a security policy statement endorsed by the current agency head. One agency had revised its security policy statement and was in the process of getting senior management endorsement at the time of the audit. For the remaining four agencies, three needed to revise their security policy, and obtain senior management endorsement. These three agencies indicated that they were in the process of obtaining current senior management endorsement.

2.58 All agencies had developed, or were in the process of drafting, a security plan or manual. All agencies had some supporting procedures. However, many of these agencies' security plans or manuals did not evidence senior management endorsement.

2.59 Six agencies did not have a document that satisfied all the requirements of a SSP as outlined in the PSM. For example, four agencies did not include a reference within their security documents to the security classification of the various areas within their premises, and the different security requirements based on those classifications (the impact being felt as threat level requirements were applied uniformly without due consideration to the sensitivity of an area). However, five of the six agencies could develop an SSP with relatively little effort.

2.60 Five agencies needed to review their security documentation in light of recent risk reviews or administrative changes. Four agencies were also unable to provide complete and/or current site maps of their premises.

2.61 Agencies also generally needed to improve the links between their key corporate, security, safety, emergency management[25] and risk policies and documents. It was not always apparent where to find guidance on a particular issue. This increases the likelihood that staff are not aware that a standard or procedure exists, and therefore do not apply the agency's standards for security. It may also lead to inconsistent application of controls, thereby exposing the agency to the risk the control was designed to minimise.

2.62 Security documentation in five of the agencies referenced relevant external government policies such as the Public Service Act, Crimes Act, Freedom of Information Act, and Privacy Act. However, the ANAO noted that the security policies and procedures of most agencies contained some inconsistencies with Commonwealth requirements, specifically those outlined in Part E of the PSM. Some of these inconsistencies had arisen as a result of the agency not reviewing its policy and procedures in light of new or revised guidance.

[25] Detailed findings in relation to safety and emergency procedures can be found in Chapter 3.

Education and awareness programs

2.63 Security only works effectively if everyone involved in adhering to the requirements are aware of their responsibilities, and consistently apply the identified controls. Agencies are required by the Commonwealth to ensure that their staff, contractors and clients are made aware of, and are regularly debriefed on, the security requirements of the agency.[26]

2.64 Agencies should develop education and awareness programs based on the security standards and documented procedures of the agency. These should be communicated to staff when they commence with the agency, and then on a periodic (at least annual) basis thereafter as part of a security refresher awareness program. Ideally, agencies should give consideration to the nature and level of involvement of their staff in certain activities to determine what training is relevant to each staff member (including any special requirements for security personnel). Agencies can also make use of information circulars to advise staff, in a timely manner, of new or revised standards.

Agency findings

2.65 Five agencies had sent their security personnel on protective security and risk management training courses conducted by the PSCC. These agencies also provided their security personnel with the necessary support to:

- attend industry conferences (such as the Security-In-Government [SIG] conference convened annually by the Attorney-General's Department); and/or
- network with peers.

2.66 The remaining two agencies had provided their ASAs with limited security and risk management training. However, these agencies had identified the need to train their ASAs, and had commenced planning for this process.

2.67 The ANAO found that four agencies did not provide their new starters with any security awareness training. In addition, ongoing security training for non-security personnel (staff) in five of the agencies audited was found to be insufficient, of a low quality and not provided to all staff. Only two agencies provided regular updates/awareness training sessions to remind staff of security requirements. The ANAO notes that the Commonwealth Protective Security Survey of 2001 confirmed this was an issue for agencies in 2001.

[26] Refer to paragraph 2.5 of Part E of the PSM, p. E8. Also refer to discussion under the Safe work environment sub-component heading of Chapter 3.

2.68 These factors contribute to an undermining of the security environment in the following ways:

- staff are unaware of the appropriate actions to take in the event of an emergency or when dealing with unacceptable or threatening behaviour. They may therefore place themselves, others or the agency at risk;
- physical security procedures and controls may be compromised as staff are not aware of the requirements in relation to these, or how to apply them;
- staff may not appropriately store, transfer or dispose of classified information as they are not aware of the storage, transfer or disposal requirements for classified material (especially when working outside the office). They may therefore place the integrity and confidentiality of the information at risk; and
- staff may injure themselves or damage agency property as they are not aware of safety and security requirements.

2.69 The ANAO also found that two agencies had developed sound procedures to inform clients[27] of their obligations, and also monitored them to ensure they complied with the requirements. However, in four agencies, the ANAO found that procedures needed to be tightened to ensure that clients were aware of the agency's security measures and/or emergency procedures. The ANAO noted that one agency had suffered several breaches of the visitor control requirements (visitors not being escorted) even though the procedures surrounding visitors were sound. This was primarily due to staff not applying standards as required, which may have occurred due to a lack of awareness.

Recommendation No.3

2.70 The ANAO recommends that agencies develop and document comprehensive, consistent and logically referenced security plans and procedures.

2.71 Agencies should also develop and schedule periodic formal education and awareness programs for non-security personnel addressing agency security standards. In addition, agencies security personnel and contractors should receive regular protective security and risk management training to ensure that they are sufficiently skilled to fulfil their responsibilities for security.

[27] Clients refer to persons not employed by the agency, who visit the agency's premises. This may include the public or other Commonwealth agency officials.

2.72 When developing security documentation, and education and awareness programs, agencies should ensure that they provide staff and contractors with adequate guidance on how to adhere to, and apply all of, the control mechanisms and procedures adopted by the agency.

2.73 Education and awareness are critical components of the security management control framework. They help to ensure that staff adhere to agency standards and expectations for security. Better practice suggests that agencies should provide staff and contractors with annual refresher courses on security. In addition, the IT division should provide an IT induction program for staff and contractors, or incorporate their training program into the general security education program.

2.74 In particular, staff and contractors should be made aware (or reminded) of their responsibilities or controls in the following areas:[28]

- information classification, handling and storage requirements. Agencies should refer to the table provided on page E49 of Part E of the PSM for guidance on the appropriate grade of security container for classified information storage, and maintain accurate records of their stocks (and placement) of security containers to facilitate management of these. Supervisors also require guidance on how to counsel staff that breach these requirements;
- access control, pass and key management standards;
- requirements for the management of visitors;
- additional, or special, procedures to be applied outside standard operational hours;
- procedures to take to deal with contact by the media or other interest groups;
- guidance on differing security requirements or actions expected of staff under the various levels of alert; and
- IT security and system usage requirements.

2.75 For decentralised operations, the ASA could work with local staff to ensure that, where they use the agency-wide program, the program is tailored to individual site requirements, or, if they develop their own training, that it is adequate and consistent with agency-wide requirements. For agencies that share premises with other building occupants, controls need to be implemented to ensure that they comply with the individual agency's requirements for security.

[28] Which are discussed in greater detail in Chapter 3.

Conclusion

2.76 The ANAO concluded that a number of agencies in the audit had established a relatively sound physical security control environment. However, there were a number of opportunities for improvement across most agencies covered by the audit. These improvements should translate into a more effective and efficient security management control framework for the agencies which adopt them.

2.77 Agencies generally performed well at assigning responsibilities for security, establishing lines of communication between their senior management and security personnel (including IT security), and maintaining current SRAs. Notwithstanding this, agencies can generally improve the delegation of security responsibility to agency staff, contractors and clients, or under decentralised or shared operating environments. In addition, agencies can be more thorough in the conduct of their SRAs, analysis and documentation of decisions and development of security documentation. A control environment is only as strong as its weakest point. If the SRA process is inadequate or key stakeholders feel that they have no obligation to uphold (or are unaware of) the agency's security standards, the security environment is likely to be compromised.

2.78 In particular, agencies need to ensure that all relevant security risks are identified and adequately considered on the basis of likelihood, consequence and agency risk tolerance. Agencies should be mindful that poor quality analysis and documentation will limit their opportunity to efficiently alter their arrangements in the event of heightened or lowered threat levels, as they would need to re-perform the assessment process in detail again to determine the most appropriate mix of controls and procedures.

Summary of Sound and Better Practice Observations

2.79 This audit identified a number of examples of sound and better practices in the agencies reviewed. A summary of these is provided in Table 2.

Opportunities for agencies

2.80 Based on the sound and better practice observations, the ANAO has identified two opportunities for the enhancement of security performance when agencies are establishing their security control frameworks.

Opportunity No.1

2.81 ***The ANAO encourages agencies to document the assigned responsibilities under their protective security control framework, and establish and enforce clear lines of accountability for critical tasks. Periodic review of responsibilities and reporting against accountabilities is also an important part of this process.***

Opportunity No.2

2.82 *The ANAO encourages the governing body for security to be proactive in its oversight of the establishment, management and maintenance of the agency's security control environment. Specifically, agencies ought to implement a process that enables the governing body on security to consider, in a thorough and logical manner, the findings and recommendations from incident, protective security risk, security and related administrative process reviews. It is desirable for the governing body to improve both the effectiveness and efficiency of the security control framework.*

Table 2

Sound and Better Practices for Establishing a Security Control Framework

Roles and responsibilities
All agencies had appointed an SES officer as the security executive, and were reporting on security management matters to a governing body.
Three agencies had developed detailed documentation on the delineation of responsibilities for security, and had clearly explained the associated tasks.
Five agencies had a statement in their key security documentation indicating that all agency staff were active participants in upholding security standards.
In all agencies, the ASAs had access to senior management and were able to make a contribution to the security decision-making process.
All agencies understood the value of seeking the assistance and advice of security experts when selecting security products and undertaking assessments.
Security risk management
Two agencies had linked the security risk register, used to monitor the protective security threats and risks of the agency, to their agencies' overall risk management framework.
Two agencies evidenced that they had a robust, iterative and integrated security risk management framework in place.
Documentation of policies, standards and expectations
Two agencies had a security policy statement that had been endorsed by the current agency head.
Five agencies had referenced the relevant internal and external requirements for protective security within their security documentation.
One agency had developed extensive security documentation that was thoroughly cross-referenced and revised at least annually.
Education and awareness programs
Five agencies had provided their security personnel with protective security and risk management training.
One agency had developed extensive security induction education, and annual refresher training, programs that were revised at least annually. It also ensured that all staff had the opportunity to attend training and provide feedback on the content.
Two agencies had sound procedures in place to inform clients of their security obligations, and monitor them to ensure that they complied with these requirements.

3. Components of a Sound Physical Security Environment

This chapter outlines the components of a sound physical security environment as outlined in the PSM. These components include a safe and secure work environment, controls and procedures for the protection of official information, assets, personnel and clients, adequate arrangements for dealing with emergency situations that arise as a result of acts of violence, and guidelines for the security of conferences and other sensitive events. The importance of documented procedures is also explored. Recommendations and opportunities for improvement identified in the agencies audited are discussed. In addition, a summary of the sound and better practice observations made during the audit is provided at the conclusion of the chapter.

At the conclusion of this chapter, there is also a brief discussion of whether the agencies in the audit had considered the physical security implications of home-based work.

Introduction

3.1 The elements of an agency's physical security environment should be designed to prevent, detect and/or respond to events that may cause harm, or allow unauthorised access, to agency staff, clients, assets and/or official resources.

3.2 This is achieved through the development and implementation of a series of key controls and procedures. These should be commensurate with the assessed level of threat, risk, resource value, information classification, and site characteristics. They should also be capable of deterring and detecting attempted breaches, and provide agency security personnel with the information they require to assess and communicate the necessary actions to prevent a crime, or minimise its consequences.

3.3 The overall objective for the agency is to implement a series of controls and procedures that will create a delay to the offender equal to the time it would take to initiate an appropriate response to the identified breach, while satisfying the minimum standards established in Part E of the PSM.

Commonwealth Guidance

3.4 Each Commonwealth agency is required to determine the appropriate level of physical protection (controls and procedures) for its functions and official resources. Section 5 of Part E of the PSM outlines the requirement for Commonwealth agencies to provide an adequate level of physical protection from harm or work place-related injuries (as outlined in the *Occupational Health* *and Safety* [OH&S] *(Commonwealth Employment) Act 1991*) for the agency's staff and clients.[29] In particular, Part E is concerned with minimising the potential of harassment to agency staff and clients.[30]

3.5 An agency should also consider arrangements for responding to emergencies that arise as a result of acts of violence, particularly bomb threats, as well as specific arrangements for conferences and other events where classified information, agency staff or other official resources may require protection.

3.6 Part E of the PSM indicates that the physical security environment is also concerned with protecting the integrity, availability and confidentiality of classified and official information. Section 7 of Part E of the PSM is devoted to this objective, and is tightly cross-referenced to Part C of the PSM (titled *Information Security*).

3.7 In addition to the guidance provided in the PSM, agencies' ASAs and ITSAs are required to consider other relevant guidance such as that provided in the Handbook 14 of ACSI 33 (issued by DSD), and the Australian Standard 3745-1995: *Emergency Control Agency and Procedures for Buildings* and the publication *Non-stop Service: Continuity Management Guidelines for Public Sector Agencies*.[31] Industry conferences and information sessions run by agencies including the PSCC and ASIO, may also provide ASAs and ITSAs with invaluable guidance and assistance when designing and implementing physical security controls and procedures.

Application of Commonwealth Guidance by agencies

3.8 As mentioned in Chapter 2, prudent management of security risk will involve finding the most appropriate and cost-effective way of minimising risk through a combination of physical, personnel and administrative measures. Protective security measures can be applied through one, or a combination, of three methods. These are outlined in the Table 3.

3.9 The advantage of adopting a mix of protective security measures, as is the case for the security-in-depth (SID) method, is that a mix provides a more effective, and less intrusive, series of controls than the application of just one type of protective security measure (for example, physical barriers). In addition, the agency would achieve greater benefits if it designs security controls and procedures that are generated from the function or resource requiring protection (as identified during the security risk assessment).

[29] Refer to paragraph 5.1 of Part E of the PSM, p. E19.

[30] By harassment, the PSM is referring to swearing and abusive language, threatening behaviour or actual physical harm, or damaging property. Refer to paragraph 5.2 of Part E of the PSM, p. E19.

[31] Also refer to pp. A24 and A25 of the PSM.

3.10 The agency should document supporting statements on its adopted controls in its security procedures, or equivalent, for use by the security personnel and staff. The agency should also provide staff with ongoing education and awareness programs on their obligations to adhere to, and apply, the security standards. For further detail on these programs refer to Chapter 2.

Audit findings—Components of a Sound Physical Security Environment

3.11 This section provides some background information on each of the four components the ANAO examined when considering agencies' security controls and procedures. A discussion of the findings in the seven agencies audited is then provided to highlight:

- examples of sound and better practices; and
- opportunities for improvement.

Table 3

Methods to Apply Protective Security Measures[32]

Method	Description
Security-in-Depth (SID)	A system of multiple layers in which security counter-measures are combined to support and complement each other, making unauthorised access by an external intruder or staff with no need-to-know difficult. These layers include a combination of physical barriers, administrative procedures and personnel security. For instance, guards, classification of information and vetting of staff.
Crime Prevention Through Environmental Design (CPTED)	This method aims to deter crime by increasing the likelihood of detection and apprehension. This method uses physical barriers to limit criminal opportunity and manipulate human behaviour. This is achieved through intensifying the detection or exposure areas to eliminate concealment, improving the response time following detection, minimising the escape routes available, and projecting to possible offenders the perception that there will be too high a level of resistance (or too likely a chance of observation) by staff or building occupants. The types of barriers employed may include lighting, fencing, building design, location, and the type of materials used (doors, windows and locks).
Concentration	A method that focuses on achieving the most cost-effective protection of assets by co-locating sensitive or high-value assets in an area, building or floor of a building, thereby limiting the potential cost of protective security measures to one site.

[32] Source: PSCC Protective Security Course 3/02 Training Materials.

Methods used by agencies

3.12 The ANAO found that all agencies had used the SID method by implementing a series of procedural, personnel and physical measures. Five agencies also provided evidence that they had applied the principles of CPTED. Another agency provided evidence that it had used all three methods by co-locating its most sensitive resources.

Components of the physical security environment that require controls and procedures

3.13 Part E of the PSM states that agencies need to document their requirements and standards for security procedures and controls in relation to the following components of the physical security environment.

Safe work environment

3.14 Commonwealth guidance on this element of the security control framework focuses on the need to provide staff with a sense of security when at work, so that they can perform their duties to the best possible standard. Equally, clients of the Commonwealth should feel safe and secure in their dealings with Commonwealth agencies.

3.15 Agency staff or clients can be placed at risk due to the nature and type of functions undertaken by the agency, or as a result of a position they hold (for example, public office holder). This risk is typically realised through the affected party being the subject of harassment. By undertaking a thorough protective security risk assessment,[33] an agency should be able to identify its, and its staffs', particular exposure to harassment and other types of risk. Whilst it is not possible to eliminate completely the risk of harassment or harm when at work, agencies can plan for, and establish adequate facilities, supporting procedures and reporting mechanisms to deter such events and/or resolve incidents in a timely manner.

3.16 The PSM stresses that the most effective method of protection (and incident minimisation) for an agency is for it to maintain a high level of security and incident response awareness amongst its staff (this concept is discussed in detail in Chapter 4). In the event of an incident, staff should ensure that they do not take any action that could endanger themselves or others. This means that an agency has to provide regular security briefings, education and documented procedures to all staff, not just security personnel.[34] The professionalism and personal behaviour of agency staff can also have an impact on client behaviour. Therefore, the PSM recommends that all staff receive training in client management techniques.

[33] Refer to *Security Risk Management* section in Chapter 2.

[34] Also refer to discussion under the Awareness and education programs sub-component heading in Chapter 2.

3.17 Another crucial aspect to consider for this component is whether the agency's site(s) and layout present any specific vulnerabilities. For instance, using the CPTED method described above (in Table 3), an agency may create delineation between public and non-public areas of the agency, install monitoring devices to record client interactions, and rely on the presence of security personnel to deter undesirable behaviour. Paragraph 5.10 of Part E of the PSM outlines a number of other factors that the agency should consider when undertaking their protective security risk assessments for this element of the physical security environment.

Agency findings

3.18 The ANAO found that all agencies audited had implemented some controls and procedures designed to ensure the safety (physical and OH&S) of their staff. Three of the agencies had particularly robust (and quality endorsed) OH&S and safety management systems in place due to the nature and type of their business functions. In addition, two of these agencies were subject to regular assessments by external regulators. Most staff across all agencies in the audit felt that the OH&S arrangements at their agency were sufficient for their needs.

3.19 The ANAO found little documented evidence that staff safety, and in particular protection from harassment, had been covered by agencies in their non-security personnel's security documentation. Three agencies had documented their procedures on harassment elsewhere, for instance in the emergency management or human resource management procedures. However, only one of those agencies had referenced its harassment procedures to its security procedures.

3.20 All agencies had some controls within their work areas to minimise access by the public to agency staff and resources. Five agencies had documented evidence to suggest that they had considered the delineation of public and non-public areas in a strategic manner (but this documentation did not always contain a reference to the need to physically protect staff).

3.21 All agencies indicated that they relied on their security personnel (who were generally from contracted-in guarding services) to apply the procedures relating to unacceptable behaviour (as outlined in paragraphs 5.37 to 5.40 of Part E of the PSM). However, the ANAO found that, in three agencies, the security personnel were not always in a position to respond to an incident as they were required to hold their physical positions, or they may have been dealing with other matters at the time of the incident. Therefore, it was left to the non-security personnel to deal with unacceptable behaviour. As these staff had not been trained adequately in emergency response or client management techniques, this would conceivably endanger their own safety.

3.22 The ANAO also found that the security personnel of two agencies did not always satisfy their staff level requirements. As well, security personnel at another agency did not always perform their designated duties, leaving their agencies exposed to the risks they were employed to manage. The ANAO notes that all agencies had taken some form of remedial action and indicated they would continue to monitor the security personnel's actions.

3.23 Of the agencies audited, three agencies that were co-located with other agencies. Of these, one had physical barriers that separated its offices from the agencies that it shared a building with, and as a result, had limited dealings with its co-tenants. The other two agencies shared a site and had joint responsibility for administering the security for that site. These agencies had developed a series of Memorandums of Understanding (MOU) outlining responsibilities between them and with other building occupants. However, the ANAO noted that many of these agreements were several years old, and needed to be revised in light of changes to the protective security risk environment and/or agency structure.

Recommendation No.4

3.24 The ANAO recommends that agencies ensure that their security risk assessment process, implemented security controls, and documented security procedures, adequately address all staff safety concerns as discussed in Sections 5 of Part E of the PSM.

3.25 The ANAO noted that some agencies had considered aspects of staff safety in their security environments. However, they had not implemented adequate controls to mitigate the risks, or appropriately educated their staff.

3.26 Given that some agencies were experiencing problems with the ability of their guards to respond to emergency and security situations, the ANAO considers that agencies should revisit the nature and extent of the use of guards as a suitable control in these situations.

3.27 In addition, agencies need to ensure that any agreements relating to security arrangements made with external providers or co-tennants are structured such that all parties are accountable for the achievement of the documented standards. The agency then needs to monitor the performance of duties under the agreement, and take appropriate and timely action in the event of a breach. A weakness (including an inaccuracy or oversight) in one agreement could be sufficient to undermine an agency's total security environment.

Emergency procedures

3.28 Agencies need to assess the risk of emergency situations arising from acts of violence as part of their protective security risk assessment process. Generally, the likelihood of these types of risks is quite low. However, all agencies should have plans and procedures in place for dealing with such emergencies. These should be commensurate with the assessed level of threat at any particular point in time.[35] For instance, in the current heightened international threat environment, agencies that are exposed to foreign sourced risks should have adequate procedures in place to deal with relevant identified threats.

3.29 Varying levels of threat and the weakened security environment that arise as a result of an emergency situation, should be dealt with through the definition of alert levels. Agencies may apply one alert level uniformly across its areas or functions. However, alert levels should be applied to a particular area or function based on its current assessed level of risk. Each alert level will have a differing mix of controls and procedures designed to achieve the most cost-efficient and effective security environment.

3.30 The primary emergency situations that the ASA (and ITSA) are concerned with include:

- bomb and bomb threats;
- failure of essential and information technology services (either through deliberate or accidental means);
- fire and explosions;
- major incidents;
- acts of violence such as physical assault, hostage situations or hold-ups;
- natural disasters;
- threatening telephone calls and letters; and
- mailbombs and suspicious packages.

3.31 The agency will need to prepare supporting procedures for its staff (and educate them appropriately[36]) to ensure they are aware of the actions they must take to protect themselves and minimise the potential impact of an identified situation. The procedures should outline the agency's requirements for safety and security, preservation of the crime scene, post-incident investigation and debriefing, and evacuation procedures.

[35] Refer to paragraphs 6.10 to 6.13 of Part E of the PSM, p. E30.

[36] The level and nature of education varies depending on the employee's responsibility in a particular emergency situation. For instance, most staff require internal training on the agency's evacuation procedures in the event of a bomb threat. However, depending on the agency's risk assessment, the fire wardens, emergency personnel and security personnel may require specific training from an external expert such as the Australian Bomb Data Centre.

3.32 The PSM provides specific procedural guidance on some of the emergency situations and matters discussed above. It also recommends that the ASA (or ITSA) refer to other relevant guidance and publications, or seek the assistance of emergency management experts. The guidance provided in the PSM is not intended to be exhaustive, as it is not the primary responsibility of the ASA (and ITSA) to be the agency's emergency management expert. However, the security environment must be adequately maintained during emergency situations. Therefore, the ASA (and ITSA) need to work with the agency's emergency management staff to ensure that they incorporate the agency's security standards (as set out in the security policy, plans and procedures) into the emergency procedures.

3.33 Agencies should also maintain records of emergency incidents, as they would for security incidents (as discussed in Chapter 4). These records should be based on timely incident reports, and used by agencies to assess the effectiveness of the procedures implemented and assist with identifying ways to improve the emergency and security arrangements.

Agency findings

3.34 The protective security risk assessments for all agencies in the audit discussed matters in relation to emergency situations arising from acts of violence. In addition, all agencies in the audit had developed emergency management plans and procedures for managing a range of emergencies, including acts of violence. The ASAs (and ITSAs) generally indicated that they had been involved in the development of these procedures, even if they weren't responsible for them.

3.35 Five of the agencies audited had particularly robust emergency management systems in place due to the nature and type of their work functions. Two of these agencies were subject to regular assessments of their emergency arrangements by external regulators.

3.36 The ANAO found that some agencies could benefit from broadening the extent and type of emergency guidance they provide to their non-security staff on emergency procedures. For instance, few agencies had covered security or operational arrangements in the event of a failure of essential services. Agencies could apply the guidance from other standards (for example AS 3745-1995) and publications to assist with this process.

3.37 The ANAO also found that, as a result of the events of 11 September 2001 in the United States of America, most agencies had reviewed and strengthened their mail handling procedures. However, agencies did not always ensure that the procedures covering other emergency situations (for example, hold-ups and major incidents) had been revised as part of this process. This represents a key exposure to some agencies in the current risk environment.

3.38 Five agencies conducted regular evacuation exercises and used the results of these to improve current emergency management practices. Most staff across the agencies audited felt that emergency arrangements were sufficient.

3.39 All agencies indicated that they had some level of liaison with external emergency management experts. However, this advice was generally gathered in an ad hoc manner. In addition, the type and frequency of contact could be improved so that this information could be used to the best strategic advantage of the agency.

Protection of official information and other official resources

3.40 The principles and procedures outlined in Section 7 of Part E of the PSM assist agencies with creating a suitable control environment for the protection of classified information and/or other official resources. One of the key principles of this section is for agencies to locate official information and resources away from public access, that is within a secured area that has appropriate controls (for instance, security containers). Equally important, is the need for the agency to ensure that all recipients of classified information apply an equivalent level of protection to its information.[37]

3.41 Critical to the concept of the protection of information and resources (from unauthorised access, damage or theft), is the classification of information and the limiting of access to this information to those people who have a need-to-know. These principles and their supporting procedures are more fully explored in Part C of the PSM. However, Part E of the PSM is closely linked with these procedures, as a weakness in one element of the protective security framework is likely to result in an exposure to the agency.

3.42 The practice of storing large quantities of classified information on IT systems, together with the high level of reliance on, and access to these systems has created many complex security exposures for agencies. These exposures are largely communications and technology based, and are therefore outside the scope of this audit. However, the protective security risk assessment process for the physical security environment should address the physical security of the equipment. Therefore the ANAO looked at this particular aspect in the agencies audited.

[37] Refer to paragraphs 7.8 and 7.30 of Part E of the PSM, pp. E36 and E40 respectively.

3.43 The categorisation of secure areas, as well as a definition of their characteristics, is provided in the PSM. They include Secure Areas, Partially Secure Areas or Intruder Resistant Areas, based on the types and standards of protective security measures present. These standards are summarised in Table 4. An area that does not meet any of these standards is known as an unsecured area. The purpose of applying classifications to areas is to assist with the selection of appropriate protective security mechanisms, procedures and clearances[38] for people who access that area. Also, by restricting the size of a classified area, agencies have a better chance of limiting the costs associated with maintaining the standards of that area.

3.44 Agencies can select from a variety of security controls (and equipment) to assist with establishing a secure area. These may be mechanical (locks, containers, cameras, alarms or access control systems) or people (guards, reception staff, or security conscientious staff) controls. However, as the budget for security is often limited, the ASA (and ITSA) needs to ensure that the available funds are carefully targeted to those areas of greatest risk, and that the most cost-efficient combination of controls is adopted.

3.45 The PSM provides agencies with high-level criteria against which to assess security controls. These include a consideration of the:

- threat characteristics;
- performance of the equipment in general and against threats of that type; and
- overall cost effectiveness.

3.46 The PSM reminds agencies that it is critical to consider the total cost of alternate solutions, from development and installation, to education of staff, through to maintenance and replacement. As with any acquisition, it is the whole-of-life costs that are critical. (Also refer to risk assessment discussion in Chapter 2.)

3.47 Agencies can also refer to the Security Equipment Catalogue (SEC), produced by the SCEC, or seek assistance from security consultants when selecting controls. Section 7 of Part E of the PSM provides guidance and a decision matrix[39] to assist in determining when, and what type of, external assistance they may require during this process based on the classification of the information held. Broadly, the higher the classification level of the information held, or the more sensitive the resource, the greater the degree and types of assistance required.

[38] The clearance (vetting) concept involves reviewing a staff member's background to provide a degree of assurance as to his/her suitability, trustworthiness and vulnerability from having access to security classified information.

[39] Refer to Ready Reckoner on p. E42 of the PSM.

Table 4
Summary of Secure Area Requirements

Area Requirement	Secure Area	Partially Secure Area	Intruder Resistant Area
Maximum level of classified information stored	TOP SECRET	TOP SECRET	SECRET
Security risk review	Yes	Yes	No
ASIO threat assessment	Yes	Yes	No
DSD approvals	Yes	Yes	No
Site Security Plan	Yes	Yes	No
Secured points of entry and other openings	Yes	Yes	No
Tamper-evident barriers, highly resistant to covert entry	Yes	Yes	Yes
Limiting entry to authorised persons	Yes	Yes	Yes
Appropriate security clearance for those people with frequent or ongoing entry	Yes	Yes	No
All persons to wear passes	Yes	Yes	No
All visitors escorted	Yes	Yes	No
Non-operational hours alarm or security guard patrols	Yes. ASIO-approved SCEC Type 1 security alarm or security guard patrols every 120 minutes as per paragraph 7.50	Yes. SCEC-endorsed security alarm or security guard patrols every 240 minutes as per paragraph 7.52	No
Storage of information in secure containers as per table on page E49.	Yes	Yes	No
Regular compliance reviews	Full	Moderate	No

3.48 The remainder of Section 7 provides guidance and criteria for agencies to use when developing procedures in support of their security controls. This includes guidance on:

- security containers;
- combination settings;
- key control;
- access control;
- visitor control;
- entry by media;
- entry and exit searches of bags;
- the role of guards and security attendants;
- security alarms;
- closed circuit television;
- security lighting; and
- office security.

3.49 As discussed previously, the agency needs to document its understanding of the security controls. This will assist with comprehension, enforcement, maintenance and monitoring (which are discussed in greater detail in Chapters 2 and 4). The PSM recommends that agencies document this information in an ASP and SSP.

Agency findings

Information security

3.50 The security risk assessments of all agencies in the audit had identified the protection of classified information or other official resources (from unauthorised access, damage or theft) as a moderate to high-level risk. Accordingly, agencies had implemented a number of controls and developed a number of procedures to address these risks. However, it was not always clear on what basis an agency had made its decision to adopt the controls it had implemented (this finding was also discussed in Chapter 2).

3.51 Six agencies in the audit had documented procedures explaining the classification, storage and handling of security classified or official information. These were generally available to staff in the security plans and/or supporting procedures. However, the ANAO found that one agency did not provide sufficient advice to its staff on information security procedures and controls (particularly in relation to electronic-based classified information). As well, four agencies had guidance that was outdated. In four agencies, low staff awareness increased the likelihood that classified information was inappropriately stored and handled.

3.52 Two agencies enforced a clean desk policy designed to support the need-to-know principle. Four of the remaining agencies made reference to the need-to-know principle, but did not actively enforce a clean desk policy, or other suitable information security procedures, to support this principle.

3.53 Two agencies required staff to sign for transfers of sensitive or classified information. However, the remaining five agencies in the audit could not evidence that they had adequately considered how to control the flow of classified information into, and out of, the agency. As a result, these agencies did not have appropriate controls and procedures in place to record transfers, or to ensure that the recipients of classified information were appropriately cleared and/or aware of the proper storage requirements for that information. The ANAO noted that this was also a significant issue for agencies in the Commonwealth Protective Security Survey of 2001.

3.54 One agency relied on its secure networks to protect the transfer of electronic-based classified information. This agency, and another three agencies, also minimised the risk of unauthorised disclosure or transfer of classified information by only permitting classified information up to the IN-CONFIDENCE level to be stored on the general network.

3.55 However, three agencies could not demonstrate that they had adequately considered the security of electronic-based classified information by establishing a direct link between the security standards and the IT security standards. Agencies generally assigned the responsibility for core business system security to the IT division. However, few agencies had established service level agreements (with business requirements and performance standards) between the IT and business divisions. This created an accountability issue, which leads to a weakening of the security environment.

Area classifications

3.56 Only three agencies had documented any objective discussions regarding the classification of their work areas. Other agencies suggested that their areas were 'secure' but this was not based on an objective assessment against the criteria established in Part E of the PSM.

3.57 Six agencies did not provide their staff with an adequate grade of storage container based on the level of classified information held, and the classification of the work area. Reasons given by agencies for having this deficiency included the cost of acquiring security containers and/or a lack of awareness of this (as well as the area classification) requirement. The Commonwealth Protective Security Survey of 2001 found that this was also an issue for a number of respondents.

3.58 Six agencies exhibited a number of desirable controls in relation to the security of their main computer rooms. However, only three agencies indicated that they actively considered the requirements of ACSI 33. These agencies did not apply all of the requirements as they found them impractical or too costly to implement. The ANAO notes that ACSI 33 is currently being reviewed.

Other physical security procedures and controls

3.59 All agencies covered by the audit use a combination of human and electronic mechanisms[40] to protect their premises, including; guards; access control systems; cameras; locks; shredders; and alarm systems. These generally form an effective system of controls.

3.60 The PSM encourages agencies to move from away from the use of security guards to electronic mechanisms.[41] However, the ANAO found that all agencies in the audit use guards in addition to electronic mechanisms. Three of the agencies rely heavily on guards to maintain the physical security environment, three rely moderately and one uses the guard primarily as a reception staff member. The guards typically supplement the electronic controls used by the agencies. In some agencies, the electronic controls (for example building access control) are disabled while the guards are on duty.

3.61 Another matter noted by the ANAO was that, in three agencies, the guards did not actively enforce the security requirements. This meant that the agency was exposed to the risks the arrangement was intended to protect it against. In other agencies, the guard was sometimes pre-occupied with a task and was not able to enforce all of the security standards. This occurred even though the agencies had generally prioritised and documented the duties expected of their guards.

[40] Mechanisms refers to electronic devices and security equipment such as electronic building access control systems, cameras and security containers.

[41] Refer to paragraph 1.9 of Part E of the PSM, p. E6.

3.62 While all agencies had mechanisms that could activate a response to a breach (for example unauthorised access to the premises), there was not always enough security personnel to effectively respond to the breaches. This was due to the limited number of security personnel used, and the fact that they were expected to respond to breaches in addition to undertaking a number of operational and management duties. For instance, a number of agencies only had one or two guards (that had to hold their position to monitor the alarms and cameras) and an ASA (who was typically occupied with other tasks). This has lead to a practice where staff (who are untrained in security practices) are having to respond to alarms.

3.63 The ANAO found that the access control systems (all agencies used some form of electronic system) were one of the key controls used by agencies for physical security. However, these were generally not designed to prevent tailgating and also were not configured to record staff movements out of areas or out of the building. Even where agencies maintain an audit trail of entry, these are not always reviewed in a timely manner. This generally limited the usefulness of this control.

3.64 All agencies required their staff to wear security passes when onsite. Staff interviews and agency walkthroughs generally identified that a small number of staff in five of the agencies audited did not always comply with this requirement even though they were aware of it. While this was not desirable, the ANAO found that it had a limited consequence in the agencies audited, as most staff were able to recognise their colleagues. However, as the ANAO only examined small and medium-sized agencies in this audit, the consequence of a breach of this type in other, larger (and/or more geographically dispersed) agencies may be significant.

3.65 All agencies had procedures in relation to the control of visitors. These procedures generally involved one or a combination of the visitor being escorted, signed in by an authorised staff member, and/or being provided with a pass to wear. The ANAO noted that staff in five of the agencies did not apply the visitor procedures at all times. For instance, visitors were not always escorted as required in the security procedures. The Commonwealth Protective Security Survey of 2001 found that this was also an issue for a number of respondents.

3.66 Better practice agencies in this audit 'attached' the visitor to the responsible staff member within the access control system to ensure that the visitor was not entering areas their escort did not have permission to enter. These agencies also completed a stocktake of visitor passes at the end of each day to ensure that all visitors had left the premises and their passes had been returned.

3.67 Six agencies had inadequate controls over the monitoring and management of keys and combinations. The ANAO was not satisfied that all agencies had implemented adequate controls to ensure that staff were reporting compromises of keys and combinations to the security personnel in a timely manner. Only one agency could provide evidence that it enforced and monitored these procedures through the conduct of timely audits.

3.68 While the majority of access control and storage devices were reported to be SCEC-endorsed products, the ANAO noted that a number of these devices were not (for example, key lockable cabinets that could not show forced entry). The ANAO also found that there were insufficient controls in some agencies to identify (in a timely manner) the compromise of these devices (for instance, access logs not reviewed or unclear reporting lines for breaches).

3.69 Four agencies had some documented guidance on the procedures during non-operational hours. The other agencies acknowledged the existence of an after-hours' arrangement, but did not document the specific requirements (or whether any specific requirements were necessary).

3.70 The ANAO observed that three agencies did not carry out entry or exit searches of bags. The ANAO considers that this type of procedure could have been used by agencies to reduce the risk that classified information or official resources were being taken from the premises without proper authorisation. Only one agency required its staff to complete a form when taking computer equipment offsite.

Recommendation No.5

3.71 The ANAO recommends that agencies ensure their security risk assessments, implemented security controls, and documented security procedures adequately address all requirements for the storage, handling and processing of any security-classified information as discussed in Section 7 of Part E of the PSM.

3.72 Agencies should ensure that their documented security procedures provide adequate coverage for the protection of security-classified information. This involves implementing and enforcing the need-to-know principle for access to security-classified information located on, or off, agency premises. Consideration also needs to be given to the security of electronically stored and transferred security-classified information. This will in part rely on the use of complementary measures, including the personnel clearance system to determine access rights, and applying the principles outlined in Part C for the transmission of security-classified information. The ANAO also considers that agencies should develop and use registers to record transfers of security-classified information.

3.73 Agencies need to appropriately classify their work areas in accordance with guidance provided in the PSM. This would then enable the ASA to make an appropriate decision as to the grade of security container required, as well as the standard of other security mechanisms for each area.

3.74 ASAs need to consider how they will ensure the implemented controls are adhered to by staff, contractors and clients. To be effective, controls must be applied consistently and properly. Therefore, appropriately detailed guidance and education programs should be generally available.

Conference security

3.75 Section 8 of Part E of the PSM provides agencies with guidance on the principles and procedures to adopt when holding conferences. The guidance is also applicable to other non-standard operational events, where security classified information or other official resources may require protection.

3.76 The aims of conference security are to prevent unauthorised persons from:

- disrupting proceedings;
- endangering attendees or property; and/or
- gaining access to security classified information or other official resources that could cause embarrassment to the agency or government.

3.77 The PSM highlights that, for each conference, the agency should appoint a Conference Security Officer (CSO) to make the necessary preparations, co-ordinate proceedings and develop a Conference Security Plan (CSP). The CSO should do this with reference to the risk characteristics of the conference (for example, classification of information, profile of people attending, and venue characteristics[42]), and based on the standards established in the agency's CSP. It is necessary for the agency to develop a CSP, as opposed to applying its ASP, as the standards for security that apply to a conference may differ from the normal standards outlined in the agency's security policy, plans and procedures.

3.78 The CSO should consult with the ASA (and ITSA) as early as is practicable to ensure that all relevant protective security matters are covered in the CSP. The role of the CSO may in fact be taken by the ASA, however it is also possible that the CSO may not be a protective security expert. In addition to internal parties, the CSO should seek threat assessment and protective security advice from external parties, including ASIO, if the level of classification of the information to be used at the conference is above CONFIDENTIAL, or it is likely that demonstrations or disruptions may occur.

[42] For conferences (involving security classified information) that are to be held in an overseas venue, agencies are required to consult the Department of Foreign Affairs and Trade (DFAT).

3.79 Section 8 of Part E of the PSM also provides specific guidance on:

- pre-conference considerations (topics to cover in the CSP, site selection and inspection, and other preparations);
- duties and responsibilities during the conference (passes, guard patrols, document security, incident response and reporting, and dealings with the media); and
- post-conference considerations (destruction of passes, transport of classified information, and reporting to internal and external parties as required).

Agency findings

3.80 Six of the agencies audited were likely to either host, organise, or let rooms on their premises for technical and other sessions where attendees would have access to classified information or other official resources. However, the ANAO found that only three agencies had prepared guidance or a policy on conference security. The remaining four agencies indicated that they did not have an immediate need to develop a CSP as it was unlikely that official information or resources would be present at the conference or session.

3.81 One agency had developed a generic CSP that was compliant with the requirements of Section 8 of Part E of the PSM. In this agency, the ASA generally took the role of CSO where required. The conference guidance and policies prepared by the other two agencies did not cover all of the requirements outlined in the PSM. For example, they did not indicate that:

- a conference-specific CSP had to be documented;
- a CSO had to be appointed;
- the CSO should liaise with the ASA and/or other external parties;
- site inspections had to be performed; or
- all of the requirements in relation to information security were followed.

Other observations—Home-based work practices

3.82 As part of this audit, the ANAO also considered whether agencies had developed a home-based work policy, that required the implementation of adequate physical controls to support home-based work practices.[43] These concepts are explored in greater detail in Part H of the PSM, and are becoming more prevalent in Commonwealth agencies as flexible working arrangements and information technology support home-based work practices.

[43] As per paragraph 2.10 of Part A of the PSM, p. A10. This requires that home-based work be carried out in a suitably secure environment.

3.83 The risks to classified information when staff work from home are similar to those in a traditional office environment. However, there are some notable differences. For instance, the risk of unauthorised access by family and friends to official information is higher, as is the risk of interception of transfers of official information over public networks.

3.84 Prior to permitting home-based work arrangements, the agency should undertake a thorough assessment of the benefits and risks from permitting such practices, and develop a policy statement outlining its position and requirements. The agency should consider each application for home-based work on its merits to determine whether the:

- cost of reducing the risks to an acceptable level are reasonable;
- security clearance level of the applicant is sufficient for the nature of the work to be performed;
- applicant is suitable to work alone and outside the usual environment; and
- duration of work and classification of information is appropriate for home-based work.

3.85 To ensure that staff adhere to, and understand, agency requirements for home-based work, the guidelines and criteria should be adequately documented and made available to them. The requirements should outline the responsibilities, duties, and security requirements for home-based activities, and be supported by written approval of the suitability of the work environment. The ASA (and ITSA) should be able to undertake regular assessments of the environment to determine its ongoing suitability.

Agency findings

3.86 The ANAO found that four agencies had prepared a home-based work policy. These agencies made the policy available to their staff through the agencies' intranet, and then linked the policy to the agency's Certified Agreement. The other agencies in the audit had not developed a policy statement as they generally discouraged staff from working at home due to logistical and cost reasons.

3.87 Of the agencies that had prepared a home-based work policy, none were able to provide evidence that they it applied the policy to develop individual agreements. The ANAO was informed that this was generally due to agencies not having permitted home-based work on an ongoing basis (longer than five working days). As a result, some agencies had identified a need to develop different policy statements based on the term of home-based work (short or long term), as there appear to be few controls over short-term home-based work arrangements.

3.88 As there were no agreements to review, the ANAO was not able to ascertain whether the information technology security considerations were adequately addressed for home-based work arrangements. However, The House of Representatives Standing Committee on Legal and Constitutional Affairs recommended, in its recent report, that Commonwealth agencies needed to improve their security procedures for the approval of off-site work and the security features of portable computers.[44]

Conclusion

3.89 The ANAO found that all agencies in the audit had made use of a variety of protective security measures (physical, administrative, and/or personnel) to restrict access, and provide protection, to security-classified information, assets, personnel and clients. For example, all agencies required their staff to wear security passes, and all had some form of visitor controls and procedures. However, there were a number of opportunities for improvement across most agencies in the audit, specifically in relation to:

- the thoroughness of the risk assessment process in addressing staff safety concerns;
- cross-referencing security and emergency documentation to ensure the security environment is maintained in the event of an emergency situation;
- improving the quality and coverage of their documented procedures, especially in relation to the classification, storage, handling and transfer of security-classified information or other official resources;
- evidencing that the protective security measures to be applied at their sites are based on an objective assessment of the:

  — level of classified information held onsite;

  — classification of the areas within the agency's premises; and/or

  — differing security measures for periods of increased threat levels, or the requirements during and after normal business hours; and
- applying the security controls and procedures consistently and properly.

3.90 These improvements should assist agencies in satisfying the requirements of the PSM, as well as achieving the full benefit of the SID principle, which is to implement a mix of procedures and controls that is more effective, and less intrusive, than the application of just one type of measure.

[44] op. cit., DHOR 2002.

Summary of Sound and Better Practice Observations

3.91 This audit identified a number of examples of sound and better practices in the agencies reviewed. A summary of these is provided in Table 5.

Opportunities for agencies

3.92 Based on the sound and better practice observations, the ANAO has identified two opportunities for the enhancement of security performance when agencies are considering the components of their security environments.

Opportunity No.3

***3.93** The ANAO encourages agencies to adopt a co-ordinated approach to the development of their security (including information technology security), safety and emergency management documentation, controls and practices. The security control framework should prompt the periodic review of these documents, so that they remain current, are appropriately cross-referenced and are consistent with other security and corporate documentation, as well as internal and external requirements for security.*

Opportunity No.4

***3.94** The ANAO encourages agencies to establish, assign and document responsibilities for conference security within a Conference Security Plan (CSP).*

Table 5

Sound and Better Practices for Components of the Physical Security Environment

Safe work environment
Three agencies had particularly robust (and quality endorsed) OH&S and safety management systems in place. Two of these agencies were also subject to assessments by external regulators.
Three agencies had provided their staff and clients with a safe physical work environment.
All agencies had delineated the public and non-public work areas.
Emergency procedures
Three agencies had comprehensive and current emergency management plans and procedures for managing a range of emergencies, including acts of violence.
Five agencies had robust emergency management systems in place. Two of these agencies were also subject to assessments by external regulators.
Protection of official information and other official resources
Six agencies had documented procedures explaining the requirements for the classification, storage and handling of classified information. Two of these agencies also enforced a clean desk policy in support of the need-to-know principle.
Four agencies minimised the risk associated with the storage and transfer of classified information by only permitting classified information up to the PROTECTED or IN-CONFIDENCE level to be stored on the general network
One agency had appropriately categorised and identified the secure areas within its premises.
Six agencies had a number of desirable controls in place to protect the security of their computing equipment.
All agencies required their staff to wear security passes when onsite.
Four agencies distinguished between the security requirements for operational and non-operational hour coverage.
Three agencies ‘attached’ visitors a responsible staff member, to ensure that they were not entering areas that their escort did not have permission to enter. They also completed a stock take of visitor passes at the end of each day to ensure that all visitors had left the premises and their passes had been returned.
Conference security
One agency had developed a generic conference security plan that was compliant with the requirements of Section 8 of Part E of the PSM.

4. Maintaining a Sound Physical Security Environment

This chapter presents the key activities associated with maintaining the physical security environment. These activities include performing periodic security risk assessments and reviews, maintaining and testing security equipment and procedures, and monitoring compliance with, and the effectiveness and efficiency of, the security environment. Recommendations and opportunities for improvement identified in the agencies audited are discussed. In addition, a summary of the sound and better practice observations made during the audit is provided at the conclusion of the chapter.

Introduction

4.1 The physical security environment needs to be regularly reviewed and maintained in order to ensure its ongoing effectiveness. Therefore agencies should monitor and review their environment by:

- undertaking ongoing assessments (both internally and externally sourced) against Key Performance Indicators (KPIs) and better practice;
- revising documentation and supporting procedures based on changes to the agency context or the protective security environment; and
- testing the veracity of their controls.

4.2 These reviews and assessments should be ongoing, as threats, risks and operating circumstances are dynamic. Therefore, the agency must be able to adapt and modify its arrangements to address these changes in a timely and effective manner. Underpinning the successful maintenance of the physical security environment is an effective information management reporting system, and a proactive governing body. Commonwealth guidance, and the application of other better practice principles on monitoring and review,[45] suggest that to effectively maintain a security control environment, agencies should undertake frequent:

- security risk assessments;
- monitoring and testing of the integrity and capabilities of security equipment and procedures; and
- analysis of the various mediums of feedback on the general, as well as agency-specific, security environment to modify and improve approaches and controls.

[45] As described in the ANAO's Better Practice Guide on *Controlling Performance and Outcomes*.

Commonwealth and other Better Practice Guidance

4.3 Part E of the PSM provides some guidance on the maintenance of the physical security environment. Discussion is restricted to the need for agencies to monitor and regularly review the security risk environment, and evaluate the security plan to ensure that the treatments and strategies remain effective and cost efficient. Part E stresses that, given enough time, almost any physical security measure can be compromised. It is therefore important to re-evaluate periodically the ability of a measure to delay unauthorised access for the designated minimum period of time.

4.4 The ANAO also noted that Part A of the PSM highlights the importance of maintenance, monitoring and review in Section 2 on the *Principles of effective protective security practice*. These principles apply equally to all components of an agency's protective security control framework, and are therefore relevant to the physical security environment. Section 6 of Part A of the PSM highlights that agencies are required to conduct regular security audits and participate in, or commission, external reviews to ensure that protective security measures are being implemented efficiently and effectively.

Application of guidance by agencies

Maintaining a sound physical security environment

4.5 To effectively monitor and maintain the security environment, agencies need to assign responsibility for the conduct of reviews of controls and procedures, and report on the results of these reviews to the agency's governing body for security. The assessment of controls and procedures should be conducted by sufficiently skilled and experienced staff, to ensure the integrity of the conclusions drawn. Sufficiently detailed records of actions undertaken as part of this process needs to be kept, and issues should be presented in a timely manner through incident and/or management reports that provide the necessary contextual information to enable the ASA and ITSA to develop the most appropriate course of action.

4.6 The governing body for security should take an active interest in the conduct and findings of this work to ensure that the work adds value to the security function, and the agency as a whole. Central to effective reporting is a sound information management system, common terms of reference and clear lines for reporting.

4.7 Figure 4 illustrates the critical processes in the total protective security control framework that are relevant to maintaining a sound physical security environment. These processes are explained in further detail in the following section.

Audit findings—Maintaining a Sound Physical Security Environment

4.8 This section provides some background information on each of the four component areas the ANAO examined when considering agencies' maintenance cycle. A discussion of the findings in the seven agencies audited is then provided to highlight:

- examples of sound and better practices; and
- opportunities for improvement.

Security risk assessments and security reviews

4.9 The PSM directs agencies to develop procedures and systems based upon a regular review of security risks, incident reports and threat assessments. The importance of regular review and re-evaluation of physical security risks and controls is highlighted in paragraph 4.29 of Part E of the PSM. This paragraph specifies that agencies need to regularly review the operating environment to make sure adequate protective security measures are in place. In particular, the environment should be reassessed when threats change, an agency gains or loses a function, or when the operation of functions is moved to a new physical environment.

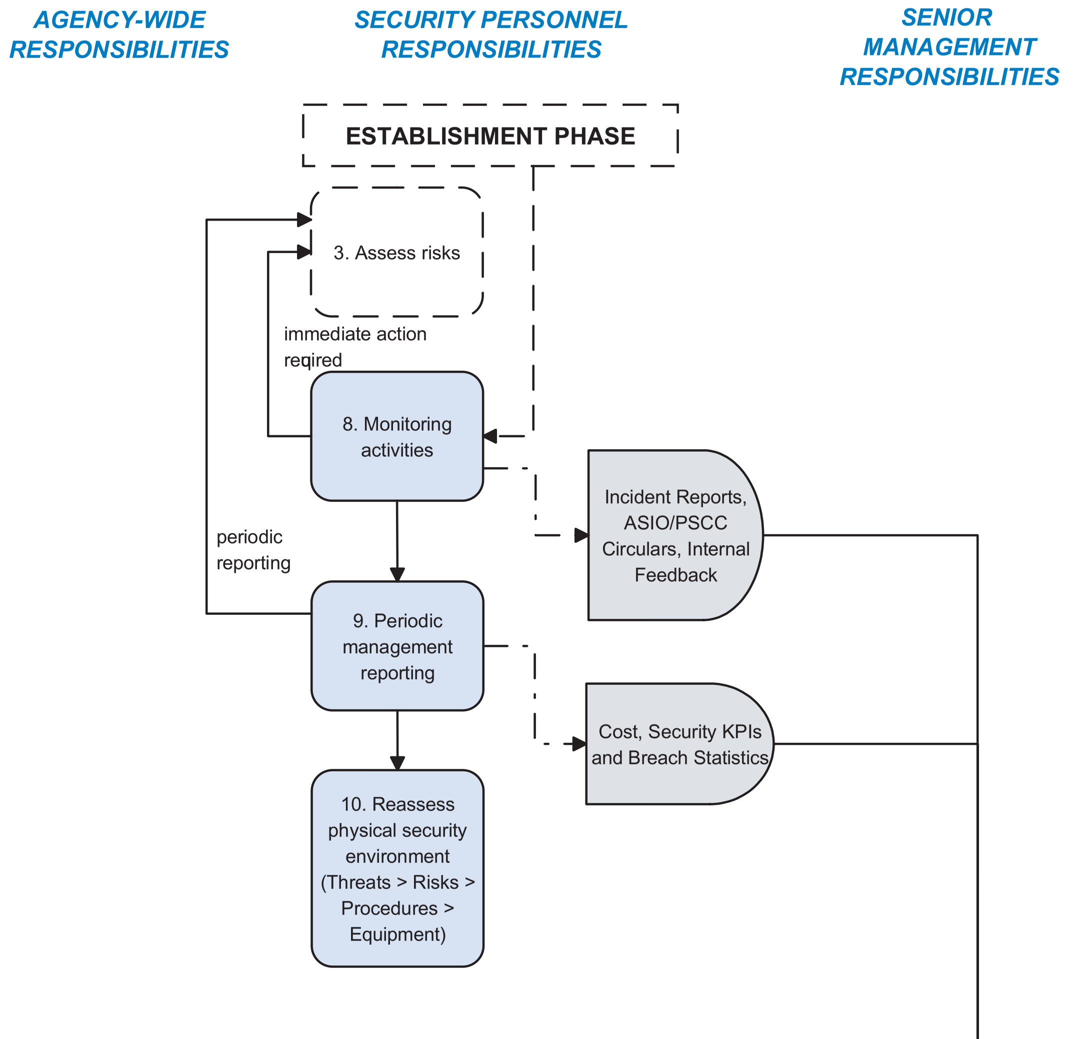
4.10 Part B of the PSM elaborates on the need to monitor and evaluate risks continuously. Agencies should consider their strategic and agency context, as well as determining their sources of potential threats to ensure that their security environment is based on a current understanding of the risks. Changes to the security risk environment may require a partial or complete security review to ensure the security plan is still relevant. In addition, periodic evaluation is necessary to ensure the effectiveness and cost-efficiency of adopted treatments and strategies.

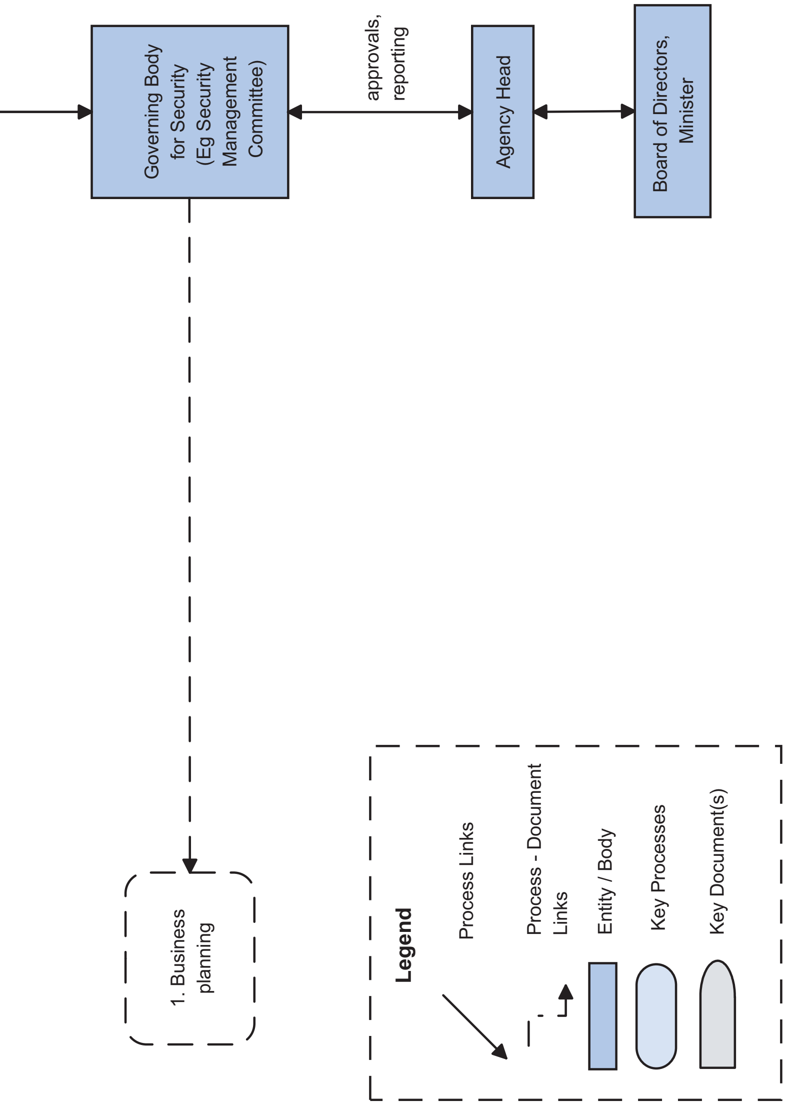
4.11 The PSM also provides agencies with guidance on determining the prioritisation of security improvements. While an allocation should have been determined during the initial security risk assessment process, agencies will need to keep detailed documentation on their decisions so that they can monitor and update mechanisms and procedures on the basis of changing circumstances.

Agency findings

4.12 All but one agency demonstrated that they were conducting regular security risk assessments. These ranged from comprehensive external assessments of the operating environment to internal assessments of one business unit's specific exposures. The agencies generally engaged external experts to assist with these assessments, and to provide advice in the assignment of responsibilities for implementing the proposed treatments. Some experts were also able to suggest appropriate education programs for the possible security mechanisms.

Figure 4
Monitoring Phase of the Security Control Framework


AGENCY-WIDE RESPONSIBILITIES
SECURITY PERSONNEL RESPONSIBILITIES
SENIOR MANAGEMENT RESPONSIBILITIES
ESTABLISHMENT PHASE
3. Assess risks
immediate action reqired
8. Monitoring activities
periodic reporting
9. Periodic management reporting
10. Reassess physical security environment (Threats > Risks > Procedures > Equipment)
Incident Reports, ASIO/PSCC Circulars, Internal Feedback
Cost, Security KPIs and Breach Statistics


Governing Body for Security (Eg Security Management Committee)
approvals, reporting
Agency Head
Board of Directors, Minister
1. Business planning
Legend
Process Links
Process - Document Links
Entity / Body
Key Processes
Key Document(s)

4.13 Four agencies had established schedules for the conduct of regular security risk assessments and security reviews. These schedules also indicated the purpose and coverage of the assessments and reviews, and were linked to the agency-wide risk management and internal audit processes. The ANAO considered that three agencies could improve the manner in which the periodic assessment of security risks and the security environment were performed. These were generally undertaken on an ad hoc basis, and had poorly defined objectives or no requirement to produce an identified deliverable. This then made it difficult for the agencies to prioritise their security improvements. Poor quality and incomplete documentation also made it difficult for agencies to learn from their experiences (this issue was also discussed in Chapter 2).

4.14 The ANAO noted that the PSCC and ASIO release regular circulars and bulletins designed to keep ASAs and ITSAs informed of changes in the threat environment. These documents also provide agencies with guidance on the recommended approach (controls and procedures) to deal with newly identified risks. All agencies indicated that they made use of this information.

4.15 In addition to the security risk assessments and security reviews, two of the agencies were subject to some form of external scrutiny from regulators. The ANAO found that this generally helped to improve their security environment and encouraged them to maintain more detailed records and documentation in support of their security environments. It also encouraged these agencies to establish clear links between the security and agency-wide management functions.

Security equipment maintenance

4.16 Agencies should develop a documented maintenance schedule for all of their security equipment. They should refer to the product developer's guidance when developing the schedule and note that for new security equipment, the maintenance terms may already be included in the warranty period.

4.17 Agencies should also ensure that maintenance work is carried out by sufficiently skilled personnel. Where these skills cannot be sourced internally, agencies should adopt a competitive tendering and contracting approach to select a maintenance provider. This should include a consideration of the cost-efficiency and technical expertise (and certifications)[46] of the provider.

4.18 The ASA should be involved in the development of any checklists used to monitor the maintenance provider's performance under the terms of the maintenance agreement. Ideally, the agreement should include provisions to

[46] For example, the agency should ensure that the maintenance provider is SCEC-endorsed, as evidence that it is duly qualified to undertake maintenance work on an endorsed security product.

identify whether a piece of security equipment currently utilised by the agency is expected to become technologically obsolete. In addition, the results of any discrepancies should be reported and acted upon in a timely manner.

Agency findings

4.19 All agencies in the audit had either outsourced the maintenance of their security equipment to external providers or developed a service level agreement with the property management area within their agency. These service providers maintain records of the security equipment specifications and maintenance requirements.

4.20 In addition, agencies generally capitalised on the experience of their service providers to assist with the development of maintenance agreements for security equipment that had not previously been covered by a maintenance agreement, or was coming to the end of its warranty period.

4.21 However, the ANAO found that the security personnel did not maintain their own records of their security equipment. In addition, some agencies did not ensure that maintenance schedules were being reviewed by the ASA. This meant that the ASA could not objectively report on the effectiveness (performance) of the implemented security products.

Review of security policies and procedures

4.22 An agency's security policy and procedures should be reconsidered on a regular basis to ensure that they address needs in the current security risk environment. The review of policies and procedures should follow directly from an assessment of the relevant security risks (as documented in a PSRR).

4.23 The security risk environment may alter making it necessary to modify the agency's attitude towards the role or importance of security. For example, events such as 11 September 2001, and more recently on 12 October 2002, have altered Australia's security risk profile. Alternatively, the agency's business operations or agency structure may change, making current policies and procedures obsolete.

4.24 The Commonwealth's protective security policy is not a static document. It has been developed to establish the Commonwealth's standards for creating and maintaining an appropriate protective security environment. As the security risk environment and Commonwealth framework alters, there is a need to revise these standards. To minimise the likelihood of a procedure losing its relevance, an agency should put in place a regular cycle to review their policies and procedures. The agency should also ensure that its policies and procedures reflect minimum Commonwealth requirements, and that any references to external requirements, and the associated terminology, are current.

4.25 In addition, the requirement for agencies to participate in the Commonwealth Protective Security Survey will assist the PSPC to determine the status of compliance with protective security in the Commonwealth. This survey, and reviews of the PSM undertaken by the ANAO, will provide invaluable insight into analysing trends, attitudes and approaches to protective security.

Agency findings

4.26 The ANAO found that two agencies in the audit had documented the requirement to review their security policy and procedures as part of the security risk assessment process. However, the remaining five agencies had not documented this requirement. Consequently, these latter agencies had security documentation that did not reflect the current security environment or Commonwealth minimum standards.

4.27 Notwithstanding this, two of the five agencies that did not document a schedule of review demonstrated that they reviewed their documentation periodically. However, the ANAO notes that this occurred as a direct result of these agencies being subject to reviews of their arrangements by external regulators. This suggests that it is necessary for agencies to document the requirement to review the security documentation, and assign responsibility for this process, in order for it to occur as required (otherwise no one is held accountable).

4.28 All agencies in this audit evidenced that they had reconsidered their security risks and documentation in light of the events of 11 September 2001. The agencies also indicated that the Commonwealth Protective Security Survey of 2001 had refocused their attention on the PSM and the standards outlined within it. However, as indicated above, these events did not necessarily give rise to an alteration of the security documentation, even when a need was identified.

Incident and management reporting

4.29 The integrity of the security environment will be strengthened where the agency proactively monitors, acts and reports on incidents that have resulted in a breach of the security arrangements. In order to establish an effective incident management and reporting system the agency needs to be aware that security threats and risks arise from sources within and/or outside the agency, and may be more or less obvious (also refer to Chapter 2: *Security risk management*). In addition, the motivation behind, and ability to access, classified information and other official resources are quite different depending on the source. These factors influence the ease and manner in which an incident may be detected.

For example, internal breaches committed, or breaches that have delayed effect, are harder to detect than breaches committed by external sources. This is primarily due to an inherent level of trust afforded to staff. Equally, incidents that have an immediate or dramatic effect may be easier to detect and report on than a covert attack.

4.30 It is crucial for the agency to respond to incidents in a structured and thorough manner. Therefore supporting procedures should be designed to assist agency staff with minimising the potential of damage or harm to the agency, or themselves, that may arise out of responding to a number of possible incident scenarios (refer to Chapter 2: *Documentation of policies, procedures and expectations* for a more detailed discussion of these procedures).

4.31 The timely recording and investigation of security incidents is crucial to the assessment of possible physical security risks. Records of incidents should be completed as soon as practicable, and maintained by the ASA. This will provide the ASA, and the governing body for security, with insights into potential areas of weaknesses, as well as enabling them to learn from past experiences. The ASA and governing body for security should aim to develop appropriate remedial measures, or revise current measures, to prevent an ongoing exposure to that risk.

4.32 The ASA will also need to harness the information collected through the incident reporting and monitoring processes to assist with reporting to management on cost and performance. This should form part of the ASA's accountability requirements, and assist the governing body for security with reporting to the agency head on the implementation of the security plan within all areas of the agency.

Agency findings

4.33 All agencies in the audit had documented a requirement to report suspected breaches of security arrangements, or the occurrence of such incidents. Six agencies had developed an incident reporting form supporting this process, and had included the relevant contact officer details. A review of these forms and the supporting records indicated a varying level of detail and review. The ANAO concluded that four of the agencies in the audit could improve the manner in which they captured and documented incident information. The timeliness of agency responses to incidents could also improve in these agencies. However, this was generally as a result of resourcing-oriented issues (insufficient staff and accountability commitments not being adequately defined).

4.34 As discussed in Chapter 2, some agencies indicated that incident reporting was part of their staff's responsibility for upholding the security environment. However, in three agencies, staff indicated that their input to the security assessment process had not been duly considered. In these agencies, the absence of sign-off and/or incomplete incident records, meant that it was not possible for the ANAO to determine whether staff suggestions had been adequately considered.

4.35 In relation to breaches by staff, the ANAO noted that most agencies indicated that repeat offenders would be punished through the withdrawal of privileges. However, the ANAO found that only two agencies enacted any form of discipline. This was generally limited to offenders receiving a debriefing from the ASA. In the better practice agencies, an attempt was made to determine the motive behind the incident. For example, if the problem was caused by a personal issue, action was taken to initiate counselling. These agencies also provided their division managers with reports every month indicating repeat offenders. The reports are signed-off by senior management, which has proven effective in heightening the effort to resolve the reported problem.

4.36 For recurring and/or significant breaches that were sourced externally, four agencies indicated that senior management would review business cases for security enhancements. These business cases would include information on the cost, benefits and performance of the proposed treatment.

4.37 Three agencies maintain a security incident database, with the results and trends identified by this facility being presented to the senior officer responsible for security on a regular basis. However only one of these agencies provided evidence that the senior officer responsible for security considered cost, performance, maintenance and incident information as a whole on a periodic basis.

Recommendation No.6

4.38 The ANAO recommends that agencies improve the procedures surrounding the reporting and recording of physical security incidents to ensure that all relevant information is captured in timely manner, and used constructively to improve the security environment.

4.39 The ASA should ensure that the agency has developed a framework for the documentation and management of incidents, otherwise the effectiveness and quality of the agency's response to incidents may degrade. The ANAO recommends that the ASA ensure the action area of incident report forms are completed so that they can be used by the ASA during his assessment of the effectiveness of implemented treatments.

4.40 Consideration also needs to be given to how security incidents will be reported on to the governing body on security and how the body uses these reports, or other review mechanisms, to the best strategic and operational advantage. Agencies could improve the effectiveness of this process by maintaining more detailed reports, and linking exceptions to treatments and action plans. This process should be documented in the revised security documentation.

4.41 The ANAO also felt that ASAs could strengthen their relationship with the ITSA (or equivalent), so that they can work together to develop adequate IT security controls. The ITSA should implement monitoring of systems and networks to ensure appropriate use of services and access to resources. Breaches of agency policy should result in revocation of privileges and/or a warning. Reports from the ITSA regarding security breaches / weaknesses may also assist the ASA to better plan for, and manage, agency security.

Conclusion

4.42 The agencies considered as part of this audit indicated that they were aware of the need to review regularly and monitor their security environments. They understood that the security environment was not static, and that it had to change in line with internal and external threats. As a consequence, most agencies undertook some form of periodic reviews and assessments of their security risks, controls and environments.

4.43 Regardless of this, the ANAO found that almost half of the agencies approached the monitoring and review of their security environment in an ad hoc manner, and were satisfied to rely on others to manage this process on their behalf. Poor quality documentation, and competing work priorities, often meant that the security personnel of an agency were unable to capture and consider all relevant information.

4.44 The information that was captured was generally not analysed to determine cause-and-effect relationships, nor was it used in a timely manner to update security arrangements. Few agencies established and reported against security KPIs, and the scope of reviews did not tend to consider efficiency issues such as the placement of equipment to best advantage. In a number of agencies, the security function appeared to be carried out in isolation from the other business support processes. In addition, many agencies showed that they had not reacted to changed circumstances or identified threats, thereby exposing them to potential serious breaches.

4.45 It was noteworthy that the two agencies that were subject to some form of external scrutiny from regulators maintained more detailed records and documentation in support of their security environments. It also encouraged these agencies to establish clear links between the security and agency-wide management functions. Therefore, it would appear necessary for agencies to document their monitoring and review requirements, assign responsibilities for these and actively track compliance to ensure that the security environment is being maintained.

Summary of Sound and Better Practice Observations

4.46 This audit identified a number of examples of sound and better practices in the agencies reviewed. A summary of these is provided in Table 6.

Table 6

Sound and Better Practices for Maintaining the Physical Security Environment

Security risk assessments and security reviews
All but one agency evidenced that they were conducting regular security risk assessments.
Four agencies had established schedules for the conduct of regular security risk assessments indicating purpose and coverage and linking this to agency-wide risk management and internal audit processes.
Security equipment maintenance
Four agencies capitalised on the knowledge of the service providers who were maintaining their security equipment by gaining their assistance when developing maintenance agreements for security equipment.
Review of security policies and procedures
Two agencies in the audit had documented the requirement to review their security policy and procedures as part of the security risk assessment process.
All agencies in this audit evidenced that they had reconsidered their security risks and documentation in light of the events of 11 September 2001.
Incident and management reporting
All agencies in the audit had documented a requirement to report suspected breaches of security arrangements, or the occurrence of incidents.
Three agencies attempted to determine the motive behind a security incident to minimise the chances for re-occurrence.
Three agencies maintain a security incident database with results and trends presented to the senior officer responsible for security on a regular basis.

Opportunities for agencies

4.47 Based on the sound and better practice observations, the ANAO has identified one opportunity for the enhancement of security performance when agencies are maintaining their physical security environments.

Opportunity No.5

4.48 ***The ANAO encourages ASAs (and ITSAs) to maintain their own records of security equipment and controls, and use these to monitor and assess these components. This would enable them to confidentially report to the security executive that these tools are being used appropriately, and they are the most effective treatment for the current environment.***

P.J. Barrett

Canberra ACT P. J. Barrett
20 December 2002 Auditor-General

Appendices

Appendix 1

Previous Audit Coverage

Audit Report No.22, 2001–2002, Personnel Security—Management of Security Clearances

The objective of this audit was to determine if agencies were managing security clearance and vetting processes effectively and efficiently and in accordance with Commonwealth policy, as shown in the Protective Security Manual (PSM).

The audit found that while security clearance policy and procedures in the agencies audited were consistent with the requirements of the PSM, there were a number of shortcomings in relation to the management, resourcing and operation of personnel security. This was typically evidenced through a backlog of initial clearances, poor clearance aftercare processes, inadequate security information management and a failure to establish and enforce (in a timely manner) appropriate re-validation procedures.

Audit Report No.7, 1999–2000, Operation of the Classification System for Protecting Sensitive Information

The objective of this audit was to assess whether Commonwealth agencies were protecting the confidentiality of sensitive information in accordance with the Commonwealth's security classification system, related government policy and standards, and recognised best practice. The audit found that none of the agencies examined were satisfying the audit objective. Key areas of weakness identified during the audit related to risk assessments and planning, allocation of responsibilities, security clearances, staff training and monitoring and review activities.

Audit Report No.21, 1997–1998, Protective Security

The main objectives of the audit were to assess the management and administration of protective security across Commonwealth agencies and to identify, recommend and report better practice in security management. The audit found inconsistencies in the identification and marking of classified information, and weaknesses in the handling and storage of classified information.

Audit Report No.15, 1997–1998, Internet Security Management

The objective of this audit was to form an opinion on the effectiveness of Internet security measures within the Commonwealth public sector and to provide better practice guidance for managing an Internet connection. The audit found that there was a lack of planning relating to policy and procedures and risk assessments, and a need for some improved controls.

Appendix 2

Audit Criteria

The ANAO established three areas of examination for this audit. These are defined and mapped against the evaluation criteria in the following table.

Areas of Examination	Evaluation Criteria
Security Framework: The agency has a security framework in place that assigns responsibilities for the identification of threats and risks, the development and management of physical security treatments and the education of staff.	• Establish whether roles and responsibilities for security have been assigned. • Determine whether the agency has undertaken an appropriate Security Risk Assessment (SRA) process prior to developing its Agency Security Plan / Site Security Plan (ASP/SSP). • Determine whether the agency has documented the requirements and expectations for its security framework. • Ensure staff are aware of their duties for security, and of the agency's security standards.
Procedures and Controls: The agency has procedures and controls in place that support its physical security framework, and these are in accordance with the agency's SRA, security policy and the minimum standards established in Part E of the PSM.[49]	• Determine whether the agency has given due consideration to providing a physically safe work environment. • Determine whether the agency has planned for, and developed, procedures that deal with emergency situations resulting from the threat of acts of violence, particularly bomb threats. • Ensure that the agency has documented standards, and physical barriers, that ensure the confidentiality and security of classified material and other official resources. • Determine whether the agency has an adequate framework in place to plan for and manage the physical security of its conferences. • Determine whether the agency has an adequate framework in place to plan for and manage the physical security arrangements for employees who work from home.
Maintenance, Monitoring & Review: The agency administers its physical security arrangements, and maintains its equipment, policies and procedures, in a timely and effectively manner, such that its security framework continues to be consistent with better practice principles outlined in commonwealth policy.	• The agency has a program in place to continuously monitor and reassess its physical security risks. • The agency should have formal maintenance agreements and a review schedule in place for all its security equipment. • The agency should have a review schedule for its security policy and procedures. • The agency should have a system in place that monitors and reports on security breaches and incidents. This reporting should contribute to the revision of the security framework.

[49] The PSM also refers the reader to other relevant guidance such as Australian Standards (including AS 3745-2002 *Emergency control organization and procedures for buildings, structures and workplaces*), as well as the *Security Equipment Catalogue* produced by ASIO on behalf of the Security Construction and Equipment Committee.

Index

Series Titles

Audit Report No.1 Performance Audit
Information Technology at the Department of Health and Ageing
Department of Health and Ageing

Audit Report No.2 Performance Audit
Grants Management
Aboriginal and Torres Strait Islander Commission

Audit Report No.3 Performance Audit
Facilities Management at HMAS Cerberus
Department of Defence

Audit Report No.4 Audit Activity Report
Audit Activity Report: January to June 2002
Summary of Outcomes

Audit Report No.5 Performance Audit
The Strategic Partnership Agreement between the Department of Health and Ageing and the Health Insurance Commission
Department of Health and Ageing and the Health Insurance Commission

Audit Report No.6 Performance Audit
Fraud Control Arrangements in the Department of Veterans' Affairs

Audit Report No.7 Performance Audit
Client Service in the Child Support Agency Follow-up Audit
Department of Family and Community Services

Audit Report No.8 Business Support Process Audit
The Senate Order for Department and Agency Contracts (September 2002)

Audit Report No.9 Performance Audit
Centrelink's Balanced Scorecard

Audit Report No.10 Performance Audit
Management of International Financial Commitments
Department of the Treasury

Audit Report No.11 Performance Audit
Medicare Customer Service Delivery
Health Insurance Commission

Audit Report No.12 Performance Audit
Management of the Innovation Investment Fund Program
Department of Industry, Tourism and Resources
Industry Research and Development Board

Audit Report No.13 Information Support Services
Benchmarking the Internal Audit Function Follow–on Report

Audit Report No.14 Performance Audit
Health Group IT Outsourcing Tender Process
Department of Finance and Administration

Audit Report No.15 Performance Audit
The Aboriginal and Torres Strait Islander Health Program Follow-up Audit
Department of Health and Ageing

Audit Report No.16 Business Support Process Audit
The Administration of Grants (Post-Approval) in Small to Medium Organisations

Audit Report No.17 Performance Audit
Age Pension Entitlements
Department of Family and Community Services
Centrelink

Audit Report No.18 Business Support Process Audit
Management of Trust Monies

Audit Report No.19 Performance Audit
The Australian Taxation Office's Management of its Relationship with Tax Practitioners
Australian Taxation Office

Audit Report No.20 Performance Audit
Employee Entitlements Support Schemes
Department of Employment and Workplace Relations

Audit Report No.21 Performance Audit
Performance Information in the Australian Health Care Agreements
Department of Health and Ageing

Audit Report No.22 Business Support Process Audit
Payment of Accounts and Goods and Services Tax Administration
in Small Commonwealth Agencies

Better Practice Guides

Administration of Grants	May 2002
Performance Information in Portfolio Budget Statements	May 2002
AMODEL Illustrative Financial Statements 2002	May 2002
Life-Cycle Costing	Dec 2001
Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	Jun 2001
Internet Delivery Decisions	Apr 2001
Planning for the Workforce of the Future	Mar 2001
Contract Management	Feb 2001
Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Managing APS Staff Reductions (in Audit Report No.49 1998–99)	Jun 1999
Commonwealth Agency Energy Management	Jun 1999
Corporate Governance in Commonwealth Authorities and Companies–Principles and Better Practices	Jun 1999
Managing Parliamentary Workflow	Jun 1999
Cash Management	Mar 1999
Management of Occupational Stress in Commonwealth Agencies	Dec 1998
Security and Control for SAP R/3	Oct 1998
Selecting Suppliers: Managing the Risk	Oct 1998
New Directions in Internal Audit	Jul 1998
Controlling Performance and Outcomes	Dec 1997
Management of Accounts Receivable	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997
Public Sector Travel	Dec 1997

Audit Committees	Jul 1997
Core Public Sector Corporate Governance (includes Applying Principles and Practice of Corporate Governance in Budget Funded Agencies)	Jun 1997
Management of Corporate Sponsorship	Apr 1997
Telephone Call Centres	Dec 1996
Telephone Call Centres Handbook	Dec 1996
Paying Accounts	Nov 1996
Asset Management	Jun 1996
Asset Management Handbook	Jun 1996
Managing APS Staff Reductions	Jun 1996