The Auditor-General
Audit Report No.23 2005–06
Protective Security Audit

IT Security Management

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 80882 1

Australian National
Audit Office

Canberra ACT
22 December 2005

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken a protective security audit across agencies in accordance with the authority contained in the *Auditor-General Act 1997*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit and the accompanying brochure. The report is titled *IT Security Management.*

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

Yours sincerely

Ian McPhee
Auditor-General

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

AUDITING FOR AUSTRALIA

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

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

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

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

http://www.anao.gov.au

Audit Team

Greg Mazzone
Martin Simon
Deborah Hope
Terena Lepper
Kristen Foster
Wayne Jones

Contents

Abbreviations

ACSI 33	Australian Government Information and Communications Technology Security Manual (DSD)
AGD	Attorney-General's Department
AGIMO	Australian Government Information Management Office
ANAO	Australian National Audit Office
DSD	Department of Defence - Defence Signals Directorate
IT	Information Technology
ICT	Information and Communications Technology
PSM	Protective Security Manual (Australian Government–AGD)

Glossary

Access Control	The process of allowing authorised usage of resources and disallowing unauthorised access.
Agencies	…includes all Australian Government departments, authorities, agencies or other bodies established in relation to public purposes, including departments and authorities staffed under the *Public Service Act 1999* (PSM 2005).
Agency Security Plan	Also known as an agency protective security plan. It is a document that contains the plan of action that the agency intends to use to address its security risks based on the context in which the agency operates and a thorough risk review (PSM 2005).
Audit criteria	Normative or desirable controls or processes (that are at reasonable and attainable standards) against which the subject matter under review is assessed.
Availability	Information systems are available and usable when required, and can appropriately resist attacks and recover from failures. Ensuring that authorised users have access to information and associated resources when required (AS/NZS ISO/IEC 17799:2001). **…** the desired state that allows authorised users to access defined information for authorised purposes at the time they need to do so (PSM 2005).
Better practice	Business practice(s) that if adopted would strengthen the internal control framework and lead to improved operational effectiveness and efficiency.
Business process controls	Policies and procedures that help ensure that the necessary actions are taken to manage risks, so that an organisation can achieve its objectives.

Confidentiality	Information is observed by or disclosed to only those who have a right to know. Ensuring that information is accessible only to those authorised to have access (AS/NZS ISO/IEC 17799:2001). … the limiting of official information to authorised users for approved purposes. The confidentiality requirement is determined by reference to the likely consequences of unauthorised disclosure of official information. The Australian Government security classification system has been developed to help agencies identify information that has confidentiality requirements (PSM 2005).
Data	Representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by humans or by automatic means.
Electronic mail (email) filtering	The objective of email filtering is to eliminate the sending and/or receipt of unsolicited mail and computer viruses that are often attached to emails.
Information	In the context of protective security, the PSM defines information as including: documents and papers; electronic data; the software or systems and networks on which the information is stored, processed or communicated; the intellectual information (knowledge) acquired by individuals; and physical items from which information regarding design, components or use could be derived (PSM 2005).
Information security	Preservation of confidentiality, integrity and availability of information (AS/NZS 7799.2:2003).
Integrity	The assurance that information has been created, amended or deleted only by the intended authorised means (PSM 2005).

IT system	A related set of hardware and software used for the communication, processing or storage of information and the administrative framework in which it operates (ACSI 33, 2005).
Protective security	A broad concept covering information, personnel, physical and information technology and telecommunication security.
Security-in-depth principle	A system of multiple layers, in which security countermeasures are combined to support and complement each other (PSM 2005).

Summary and Recommendations

Summary

Background

1. Information technology (IT) security management is an essential part of agencies' protective security environments. The management of IT security is a key responsibility of Australian Government agencies[1], and is necessary to protect the confidentiality, integrity, and availability of information systems and the information they hold[2]. Effective IT security management requires the development and implementation of an IT security control framework[3] designed to minimise the risk of harm to acceptable levels. Given the increasing reliance on the interconnectivity of Australian Government information systems, agencies have an additional responsibility to consider how their IT security environment may impact other government agencies as well as other parties with whom they share information.

2. The *Australian Government Protective Security Manual* (PSM) establishes the framework of policies, practices and procedures designed for Australian Government agencies to use in protecting Australian Government functions and official resources from sources of harm[4] that would weaken, compromise or destroy them. The PSM, which was re-issued in October 2005, identifies current standards for protective security, and specifies minimum requirements for the protection of Australian Government resources.

Audit scope and objective

3. This audit is a part of the ANAO's protective security audit coverage.[5] The objective of this audit was to determine whether agencies audited had developed and implemented sound IT security management principles and practices supported by an IT security control framework, in accordance with Australian Government policies and guidelines.

---

1 For the purposes of this report, the ANAO has used the definition of 'agency' as provided by the *Protective Security Manual* 2005, which defines agency as including 'all Australian Government departments, authorities, agencies or other bodies established in relation to public purpose, including departments and authorities staffed under the *Public Service Act 1999.*'

2 Confidentiality, integrity and availability are considered key objectives of IT security controls for protecting information.

3 An IT security control framework is the design of management processes and supporting policies and procedures, that together provide assurance that IT security management is operating effectively. Discussed further in chapter 2.

4 The PSM defines harm as being any negative consequence, such as a compromise of, damage to, or loss incurred by the Australian Government.

5 Appendix 2 provides an overview of related ANAO audits.

4. The audit at each agency examined the framework for the effective management and control of IT security, including the management of IT operational security controls and, where applicable, was based on the Australian Government protective security and information and communications technology (ICT) security guidelines that were current at that time.

Selected agencies

5. The eight agencies selected for review were:

- Australian Agency for International Development;
- Australian Office of Financial Management;
- Bureau of Meteorology;
- ComSuper;
- Department of Education, Science and Training;
- Department of the Environment and Heritage;
- Department of Immigration and Multicultural and Indigenous Affairs; and
- Department of Transport and Regional Services.

Audit conclusion

6. Overall, the ANAO concluded that the audited agencies had identified relevant Australian Government policies, practices and procedures for the protection of information. However, most agencies had not implemented structured processes to ensure the effective alignment of the IT security policy objectives with organisational risk management processes and Australian Government policy, practices, and standards for the safeguarding of information resources.

7. The ANAO found that the majority of agencies audited had adequately identified relevant external compliance obligations, and IT personnel interviewed were aware of relevant legislation and the associated compliance requirements. However, only two agencies could demonstrate suitable processes to assess system compliance with their IT security policy and with government requirements, and processes for managing exceptions/variations.

8. The ANAO found that most agencies did not maintain key IT operational procedures and configuration documentation. This was particularly evident of agencies that had contracted to third-party service providers for the provision of IT and/or IT security services.

9. The audit identified a number of opportunities for further improvement in agencies' policies and procedures relating to IT security management practices. These included:

- improving the content and processes for developing and maintaining IT security policy alignment with organisational risk management processes;
- ensuring a regular process exists within the IT security control framework to identify gaps between an agency IT environment and Australian Government expectations. This will assist in determining whether systems are operating at an acceptable level of risk;
- ensuring policies clearly identify the physical and environmental security controls and standards for managing IT equipment;
- ensuring performance reporting of network security practices are designed to ensure that security controls are adequately addressing IT security risks; and
- ensuring standards exist and are applied for the use of audit trails[6].

Recommendations

10. The ANAO has made five recommendations based on the audit findings from the agencies reviewed. Given the need for all agencies to effectively implement and manage IT security, these recommendations are likely to have relevance to the operation and management of IT security in all Australian Government agencies.

Agencies' comments

11. The eight agencies examined in the audit agreed with the recommendations.

12. In addition, the Attorney-General's Department and the Department of Defence—Defence Signals Directorate, stakeholders in Australian Government IT Security, responded positively to the audit report. DSD specifically noted that the recommendations are consistent with a fundamental requirement of the Australian Government Information and Communications Technology Security Manual (ACSI 33).

---

[6] In computer security terms, an audit trail provides a chronological record of system resource usage. It is commonly referred to as logging. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred.

Recommendations

The following recommendations are based on the findings of fieldwork at the audited agencies. The ANAO considers they are likely to be relevant to all agencies in the Australian Government sector. All entities should therefore assess the benefits of implementing the recommendations in light of their own circumstances, including the extent to which each recommendation, or part thereof, is addressed by processes and controls already in place.

IT security control framework

Recommendation No.1
Para 2.18
IT security policy

The ANAO recommends that agencies incorporate into their information security management framework, an IT security policy that establishes an agency's IT security objectives and scope, and provides reference to supporting IT security plans, procedures and standards. In addition the policy should incorporate requirements of Australian Government policies, standards and guidelines for the safeguarding of information resources.

Recommendation No.2
Para 2.34
Compliance

The ANAO recommends that agencies strengthen IT security risk processes through the use of documented IT security risk assessments, plans and policies, and conduct periodic reviews to identify gaps between agencies' IT environments, ideal risk profile and relevant government policies, standards and guidelines.

IT operational security controls

Recommendation No.3
Para 3.17
IT equipment security

The ANAO recommends that agencies improve IT equipment security practices by ensuring that physical and environmental security controls of computing resources are clearly stated as part of their IT security policy, and that responsibilities for protecting information resources are established and documented.

Recommendation No. 4

Para 3.29

Network security management

The ANAO recommends that agencies, as a part of their IT governance arrangements, monitor the effectiveness of network security practices and controls by establishing performance measures and incorporating periodic reporting against these measures.

Recommendation No. 5

Para. 3.39

Logical access management

The ANAO recommends that agencies, as a part of their system access arrangements, establish standards for the logging of inappropriate or unauthorised activity and introduce routine processes for monitoring and reviewing system audit logs.

Agencies' responses to the recommendations

13. The eight agencies examined in the audit agreed with the recommendations.

14. Agencies' responses to the recommendations are shown following each recommendation in chapters 2 and 3. Other general comments provided by the agencies are shown at Appendix 1.

Audit Findings and Conclusions

1. Introduction

This chapter provides background information about the audit scope and objective, and provides an overview of the Australian Government protective security framework and its requirement for information security. The role of IT security controls and processes for safeguarding of information is also discussed.

Information security

1.1 Information security is the protection of information and information systems and encompasses all infrastructure that facilitate its use - processes, systems, services, and technology. It relates to the security of any information that is stored, processed or transmitted in electronic or similar form,[7] and is also defined as the preservation of confidentiality, integrity and availability of information.[8] Definitions of these terms are provided in Table 1.1 below.

Table 1.1

Information Security Objectives

Objective	Definition
Confidentiality	Information is observed by, or disclosed to, only those who have a right and need to know.
Integrity	Assurance that information has been created, amended or deleted only by the intended authorised means.
Availability	Information systems are available and usable when required, and can appropriately resist attacks and recover from failures.

Source: Adapted from the *PSM* (2005) and 7799.2:2003 – *Information Security Management Part 2: Specification for information security management systems*, Standards Australia/Standards New Zealand, 2003.

IT security

1.2 IT security is a subset of information security and is concerned with the security of electronic systems, including computers, voice and data networks. It is also concerned with providing a system to establish, maintain, manage and monitor business and operational controls surrounding IT resources, in accordance with organisational information management requirements.

---

7 <http://www.dsd.gov.au/infosec/what_infosec.html>, accessed 13 October 2005.

8 AS/NZS 7799.2:2003–*Information Security Management Part 2*: *Specification for information security management systems*, Standards Australia/Standards New Zealand, 2002, p. 3.

1.3 Effective implementation and management of IT security requires both an IT security control framework and the implementation of IT operational security controls. These are defined in Table 1.2 below. The control framework provides a management structure designed to ensure that agencies take the necessary action to manage IT security risks. Operational security controls support implementation of the control framework through addressing objectives of confidentiality, availability and integrity of information or data stored or transmitted.

Table 1.2

Security controls

Control type	Definition
IT security control framework	Policies and procedures that help ensure the necessary actions are taken to manage risks, so an agency can achieve its objectives.
IT operational security controls	Processes and supporting technologies that ensure the confidentiality, integrity and availability of an organisation's information processing environment.

Source: ANAO.

1.4 The *Protective Security Manual* requires Australian Government agencies to protect information resources, including ICT systems, from compromise and misuse.[9] In addition to providing policies, practices and procedures for safeguarding government resources, the PSM directs government agencies to refer to the *Australian Government Information and Communications Technology Security Manual* (ACSI 33) for ICT security topics.[10] ACSI 33[11] outlines a combination of physical, personnel, information, IT and communications measures to assist agencies to implement IT security controls that satisfy the minimum standards required to protect information stored or transmitted via electronic means.[12]

1.5 Sound information security controls are important to enhance agencies' confidence that their recorded business transactions are valid, accurate and complete, and sufficiently mitigate the risk of information being exposed to unauthorised access.[13]

---

9 Attorney-General's Department (2005), *Protective Security Manual 2005*, Part A, para 2.4.

10 Attorney-General's Department (2005), op. cit., Part C, para. 7.23.

11 Defence Signals Directorate (DSD), *Australian Government Information and Communications Technology Security Manual* (ACSI 33), <http://www.dsd.gov.au/library/infosec/acsi33.html> The current version of the Manual was released in September 2005.

12 Additionally a number of Australian standards are useful to agencies in determining better practice requirements when developing and managing IT Security. A listing of these is included at Table 1.3.

13 Australian National Audit Office (2005), *Interim Phase of the Audit of Financial Statements of General Government Sector Agencies for the Year Ending 30 June 2005,* Audit Report No. 56 2004–05, p. 52.

Contemporary IT security issues

1.6 Management of IT security matters has received considerable attention in the Parliament, the media and among the general public in recent years. The Joint Committee of Public Accounts and Audit (JCPAA) has also drawn attention to a number of IT security issues and concerns, including:

- a lack of physical security of computing resources, in particular mobile computing resources such as laptops, personal electronic devices and backup tapes;
- the need to pursue better practice with the making and management of security contracts between agencies and external service providers; and
- a lack of knowledge of appropriate reporting requirements in the event of a security breach.[14]

1.7 A current trend in the government sector is for operations and service delivery to extend beyond traditional agency boundaries, requiring government agencies to share information and business processes with each other and, at times, with private enterprise and the general community. In order to interoperate, in a trusted and cost-effective way, it is important for agencies to use agreed technical protocols and standards[15].

Audit objective, scope and criteria

Objective and scope

1.8 This audit is a part of the ANAO's protective security audit coverage.[16] The objective of this audit was to determine whether agencies had developed and implemented appropriate IT security management principles and practices, in accordance with Australian Government expectations. It specifically considered the IT security control framework and IT operational security controls.[17]

1.9 The audit did not review agencies' policies or standards for business continuity or system development practices. The ANAO provides coverage of these controls and practices in its performance audit reports.[18]

---

[14] JCPAA, *Report No. 399 Inquiry into the Management and Integrity of Electronic Information in the Commonwealth*, 2004, Foreword, from page vii.

[15] This is known as interoperability, which is defined as: the ability to transfer and use information in a uniform and efficient manner across multiple organisations and information technology systems. See Australian Government Technical Interoperability Framework, Foreword accessed on 14 October 2005 at:
<http://www.agimo.gov.au/ publications 2005/04/ agtifv2#Australian%Technical%Framework>.

[16] Appendix 2 provides an overview of related ANAO audits.

[17] Appendix 3 provides an overview of the audit objectives and scope.

[18] ANAO reports are available from the ANAO's website. <http://www.anao.gov.au>.

Audit criteria

1.10 The performance of each agency was assessed against a set of desirable controls or better practice principles (hereafter described as the audit criteria). The audit criteria, which were developed by the ANAO, reflect the policies, standards and guidelines contained in Australian Government guidance documents (provided in the table below). In addition, the ANAO also included elements from Australian and International Standards such as the AS/NZS ISO/IEC 17799:2001 *Information Technology – Code of practice for information security management,* Standards Australia & Standards New Zealand, 2001.

Relevant documents

1.11 Table 1.3 details the relevant Australian Government guidance documents and Australian standards for managing and implementing information and IT security. The ANAO also referred to these documents when preparing the audit criteria and test program for this audit.

Table 1.3

Relevant guidance documents and standards

Government guidance documents
Australian Government Protective Security Manual, Attorney-General's Department, 2005[19].
Australian Government Information and Communications Technology Security Manual (ACSI 33), Defence Signals Directorate, June 2004.[20]
Standards
AS/NZS ISO/IEC 17799:2001 *Information Technology – Code of practice for information security management*, Standards Australia & Standards New Zealand, 2001.
AS/NZS 7799:2003 *Information Security Management Part 2: Specification for information security management systems*, Standards Australia & Standards New Zealand, 2003.
AS/NZS 4360:1999 *Risk Management*, Standards Australia & Standards New Zealand, 1999.
HB231:2000 *Information security risk management guidelines*, Standards Australia & Standards New Zealand, 2004.
13335:2003 *Information Technology – Guidelines for the management of IT Security*, Standards Australia & Standards New Zealand, 2003.
AS 8015 – 2004 *Corporate Governance of Information & Communication Technology*, Standards Australia & Standards New Zealand, 2005.

Source: ANAO

[19] Unless stated, this audit report refers to the 2000 version of the *Protective Security Manual* (PSM 2000). The Attorney-General's Department have released a revised version of the PSM, titled *Protective Security Manual 2005,* in October 2005. The Foreword states: 'The revised Manual details the minimum standards for the protection of Australian Government resources…that agencies must meet in their operations'.

[20] This audit criteria references ACSI 33 as issued in June 2004, however, references in this audit report to policies, standards or practices refer to the current version of the Manual, which was released in September 2005.

Selected agencies

1.12 The following agencies were selected for review:

- Australian Agency for International Development;
- Australian Office of Financial Management;
- Bureau of Meteorology;
- ComSuper;
- Department of Education, Science and Training;
- Department of the Environment and Heritage;
- Department of Immigration and Multicultural and Indigenous Affairs; and
- Department of Transport and Regional Services.

Audit Methodology

1.13 The audit methodology involved interviewing selected officers, reviewing policy and procedural documents, and examining documentation relating to the agencies' IT security management.

1.14 The audit was undertaken in accordance with the ANAO's Auditing Standards and was completed at a cost of approximately $333 211.

Audit Findings

1.15 The ANAO provided each agency with a discussion paper detailing the audit findings, recommendations for improvement and conclusions arising from the fieldwork specific to them.

1.16 The Attorney-General's Department and the Defence Signals Directorate were also provided with draft copies of this report prior to its finalisation, given their stakeholder responsibilities for IT security.

1.17 The audit findings are presented in chapters 2 and 3 of this report.

2. IT Security Control Framework

This chapter describes elements required for an IT security control framework and provides references to relevant Australian Government policies, practices and procedures. The chapter also discusses the audit findings in relation to the framework for the effective management and control of IT security.

IT security control framework

2.1 An IT security control framework supports management controls with the aim of ensuring IT security adequately protects information resources in accordance with agencies' information security objectives. The ANAO considers that in order to effectively manage IT security controls, agencies should:

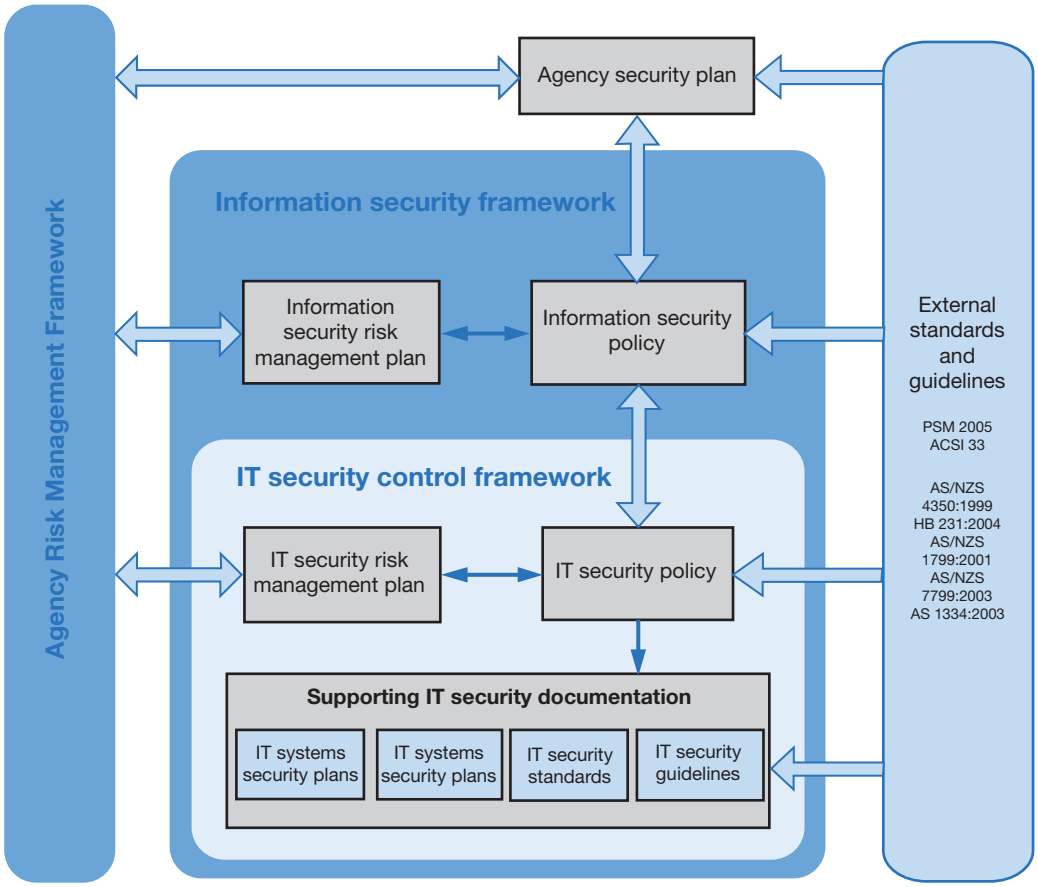
- identify and assess the risks to information resources;
- develop an IT security policy;
- treat the identified risks;
- periodically review risks and risk treatments; and
- monitor the operation and effectiveness of the security policy.

2.2 For agencies that have responsibility for Australian Government information resources, an IT security policy and security risk assessments are considered to be mandatory requirements in order to comply with the PSM and other Australian Government guidance documents. [21]

2.3 An IT security policy is an integral component of the IT security control framework. It supports the overall agency security plan by providing a link between the agency's risk management framework and information security policy objectives. An IT security policy provides the direction and support for the implementation and monitoring of suitable IT security controls. These elements are illustrated in Figure 2.1.

[21] See for example, Defence Signal Directorate (September 2005), para 2.2.4 and 2.2.5 describes mandatory security documentation requirements. PSM (2005) Part C para 7.23 states that 'ICT systems that process, store or communicate official information must comply with ACSI 33'.

Figure 2.1
IT security control framework



Source: ANAO adapted from government guidelines.[22]

2.4 A range of IT security documentation supports the IT security policy and is important for effective operation and administration of IT security. An overview of supporting documentation is included in Table 2.1.

[22] Adapted from: 13335:2003 *Information Technology–Guidelines for the management of IT Security*, Standards Australia & Standards New Zealand, 2003. Attorney-General's Department (2005), The *Protective Security Manual*, and *Australian Government Information and Communications Technology Security Manual* (ACSI 33), Defence Signals Directorate, September 2005.

Table 2.1

IT security documentation overview

Document	Purpose
Information security policy	To address at the agency level, the issues of security awareness, responsibility, behaviour and deterrence. This is a component of an agency's security plan[23].
IT security policy	To provide a high-level policy objective and is a component of an agency's information security policy.
IT security risk management plan	To identify controls needed to meet agency protective security policy. The plan has two parts: an IT risk assessment and an IT risk treatment plan.
IT system security plan	To define actions or standards for implementing an agency's risk management plan.
IT security procedures and standards	To provide instructions to system users, administrators and managers to enable compliance with an agency's system security plan.

Source: ANAO, adapted from The Protective Security Manual (2005) and the ACSI 33 Manual (September 2005).

2.5 The audit criteria, against which the adequacy of the audited agencies' IT security framework were assessed, are detailed in Table 2.2 below.

Table 2.2

IT security control framework – audit criteria

IT security control framework		
The agency has established a framework that reflects management's commitment and attitude to the implementation and maintenance of effective IT security controls, and aligns policies, procedures and day-to-day work practices with overall agency objectives for the secure management and control of each part of the IT systems. **The components in the scope of this audit, and elements assessed within each of these, are listed below.**		
Component	**Criteria**	**Elements assessed**
IT security policy	An IT security policy is documented and provides a high-level objective. The policy references existing government policy, standards and guidelines, assigns responsibilities to personnel for the management of IT security, and references other IT security plans or standards.	▪ Policy content ▪ Alignment with IT security risk assessment ▪ Review process
Compliance with internal and external requirements	Relevant criminal and civil law, and statutory, regulatory or contractual obligations, and security requirements are identified and documented.	▪ Compliance with external requirements ▪ Compliance with the Protective Security Manual waiver process ▪ Technical and compliance reviews
IT security organisation structure	An appropriate organisational structure is established to maintain security over information assets.	▪ IT security management structure ▪ Accountability for information resources

Source: ANAO

[23] Attorney-General's Department (2005), op. cit., Part C, Section 4.

2.6 These components and the respective audit findings are discussed in turn below.

IT security policy

2.7 The purpose of an IT security policy is to articulate an agency's objective and purpose for establishing and maintaining IT security controls, and to align agency information security objectives with day-to-day work practices. The ANAO reviewed the extent to which audited agencies had addressed the following elements:

- policy content
- alignment with IT security risk assessment; and
- review process.

Policy content

2.8 The ANAO expected that an entity's IT security policy[24] would include an overview of the agency's high-level IT security objectives and scope, and provide reference to other agency IT security plans or standards.

2.9 In addition, the ANAO assessed whether agencies' IT security policy was communicated to all employees, and that management from business areas were aware of their responsibility to monitor and contribute to updates should business security objectives change.

Alignment with IT security risk assessment

2.10 Australian Government guidance suggests agencies should develop a risk management plan to manage organisational risks. The ANAO considers that such a plan is important in order for agencies to identify the risk for each information asset within the scope of the IT security policy, and then determine appropriate controls for each assessed risk.

2.11 The ANAO assessed whether agencies audited undertook an IT security risk assessment for IT resources considered as essential for conducting business. In addition, the ANAO evaluated whether a clear link existed between agencies' IT security policy and IT security risk assessment. The ANAO considers that it is important for agencies to provide assurance that controls implemented to treat risks to the IT resources are based on the risk profile established through a risk assessment process, and approved by management.

---

[24] The current version of ACSI 33 (September 2005) refers to an IT Security Policy as an 'Information and Communications Security Policy'.

Review process

2.12 Regular reviews of policies and procedures assist agencies to ensure that IT security policy continues to meet organisational needs.[25] In addition, the ANAO considers that this is facilitated by defining in the IT security policy, a review process, assigning responsibilities for maintaining and reviewing the IT security policy, and specifying a timeframe for review.

Audit findings

2.13 The content of the IT security policy of approximately half of the entities assessed met the criteria for content of an IT security policy. Issues identified during the course of the audit were:

- one agency did not have a current IT security policy and one agency had an IT security policy in draft for a considerable period of time, without management endorsement; and
- three agencies' IT security policies did not incorporate reference to agency plans or standards concerning acceptable IT operational controls, such as network management or monitoring of electronic mail.

2.14 The ANAO found that most agencies had not implemented structured processes to ensure the effective alignment of the IT security policy objectives with organisational risk management processes.

2.15 The ANAO also found that while the majority of agencies specified that a periodic review of the policy was required, seven agencies did not define a review period.

2.16 The ANAO concluded that agencies' management of IT security would improve by ensuring that IT security policy adequately addresses minimum government requirements for the protection of information resources. In addition, more clearly defined linkages between agencies' IT security policy and information security policy would better support overall organisational objectives for information security.

2.17 Security better practice suggests it is important that the development of IT security policies and plans be performed in conjunction with risk assessment and treatments, both at the organisational level and the information system level, so that controls implemented to protect information resources are cost-effective and in accordance with expectations.

---

[25] See for example: Defence Signals Directorate (2005), op. cit., Part 2 Ch 2 para. 216 and AS/NZS ISO/IEC 17799:2001 clause 3.1.2.

Recommendation No.1

2.18 The ANAO recommends that agencies incorporate into their information security management framework, an IT security policy that establishes an agency's IT security objectives and scope, and provides reference to supporting IT security plans, procedures and standards. In addition, where appropriate, the policy should incorporate requirements of Australian Government policies, standards and guidelines for the safeguarding of information resources[26].

Agencies' responses

2.19 All agencies examined in the audit agreed with the recommendation. Specific comments, which were provided by the Department of Education Science and Training and the Department of Immigration and Multicultural and Indigenous Affairs, are recorded in Appendix 1.

2.20 In addition, the Attorney-General's Department and the Defence Signals Directorate agreed with the recommendation. Additionally, DSD noted that this is a fundamental requirement of ACSI 33.

Compliance with internal and external requirements

2.21 Compliance activities are generally accepted as an important component of an effective corporate governance framework. Australian Government agencies are required to identify and comply with security obligations for the protection or disclosure of information under applicable legislation.[27]

2.22 The ANAO reviewed the extent to which audited agencies had established the following elements as a part of their IT security control framework:

- compliance with external requirements;
- compliance with the *Protective Security Manual* waiver process; and
- technical and compliance reviews.

---

[26] The need for an IT security policy is currently a PSM minimum standard–Attorney-General's Department (2005), op. cit., Part C, para 4.3.

[27] Attorney-General's Department (2005), op. cit., Part A.

Compliance with external requirements

2.23 Australian Government agencies are required to identify and comply with relevant criminal and civil law and statutory, regulatory or contractual obligations with respect to agencies' security requirements.[28]

2.24 The ANAO assessed whether agencies' IT security policies clearly referenced external compliance requirements, and whether key IT personnel displayed a general awareness of external legislation and compliance requirements.

Compliance with the Protective Security Manual waiver process

2.25 An important element of compliance is the level of risk an agency is prepared to accept. Where an agency has determined it does not comply with a mandatory PSM requirement and decides to carry that risk, the agency is required to issue a waiver in accordance with PSM requirements.[29]

2.26 The ANAO expected agencies to display an understanding of the PSM waiver process and to include a mechanism for recording the waiver decision-making process.

Technical and compliance reviews

2.27 Technical compliance is the process of evaluating and monitoring agencies ongoing compliance with IT security policies and requirements. Reviews that investigate the appropriateness and adequacy of general and system security controls are key elements of agencies' continuous review process.

2.28 The ANAO assessed the extent to which agencies' IT security control frameworks referenced internal standards and requirements, and whether agencies required information systems to undergo certification and compliance reviews.[30]

Audit findings

2.29 The ANAO found that the majority of agencies audited had adequately identified relevant external compliance obligations in their IT security policy. Additionally, IT personnel interviewed were aware of relevant legislation and the associated compliance requirements.

---

[28] Attorney-General's Department (2005), op. cit., Part A. In addition, the recently released PSM states that agencies should maintain a record of any waiver issued. (Part A, para 1.14).

[29] Attorney-General's Department (2005), op. cit., Part A.

[30] The purpose of certifying IT system security is to assure management that the information system has been secured in accordance with the agency's requirements. Certification, which involves a comprehensive analysis and evaluation, is a prerequisite for accreditation. Accreditation is a formal acknowledgement by the head of the agency or their authorised delegate that the system operates at an acceptable level of risk.

2.30 Only two of the eight agencies audited were found to have established internal processes that identified IT security non-compliance with Australian Government requirements for information security, with only one agency maintaining records of submitted waivers.

2.31 Whilst the remaining six agencies displayed some understanding of the PSM waiver process, it ranged from knowing that a PSM waiver process existed to a full working knowledge. An ability to apply the PSM waiver process was also limited as they did not include in their IT security control framework, a regular process to identify possible gaps between an agency's IT environment and the PSM and/or ACSI 33. This also reduces the ability to determine whether systems were operating at an acceptable level of risk.

2.32 Two agencies had suitable processes in place to assess system compliance with their IT security policy and with government requirements. However, neither agency could demonstrate (at the time of the audit fieldwork) a routine review process as a part of the IT security control framework.

2.33 The ANAO concluded that agencies' management of IT security would benefit from reviewing relevant compliance obligations as a part of the establishment and maintenance of IT security control frameworks. The ANAO considers that agencies should also undertake technical and compliance reviews for IT security to ensure that IT systems are protecting information as expected.

Recommendation No.2

2.34 The ANAO recommends that agencies strengthen IT security risk processes through the use of documented IT security risk assessments, plans and policies, and implement periodic review processes to identify gaps between agencies' IT environments, ideal risk profile and relevant government policies, standards and guidelines.

Agencies' responses

2.35 All agencies examined in the audit agreed with the recommendation. Specific comments, which were provided by the Department of Education Science and Training and the Department of Immigration and Multicultural and Indigenous Affairs, are recorded in Appendix 1.

2.36 In addition, the Attorney-General's Department and the Defence Signals Directorate agreed with the recommendation. Additionally, DSD noted that this is a fundamental requirement of ACSI 33.

IT security organisation structure

2.37 A defined organisation structure facilitates the ability of agencies to implement, monitor and coordinate its IT security function. The ANAO assessed the extent to which agencies defined in their IT security control frameworks an IT security management structure and established standards for the ownership and accountability of information resources.

IT security management structure

2.38 The ANAO assessed whether agencies had an organisational structure in place to develop, implement and maintain IT security policy, plans, standards and procedures in line with agencies' information security requirements. The ANAO considers that clarity of the management structure for IT security is important so as to maintain a coordinated approach to security within the organisation by assigning security responsibilities and accountability for data and systems.

Accountability for information resources

2.39 Australian Government agencies are required to use risk assessments and the information security classification system to identify valuable or sensitive information and to allow information to be shared between agencies using an agreed and appropriate level of protective security.[31]

2.40 The ANAO assessed the extent to which the IT security control framework of the agencies audited addressed ownership of information resources and assigned a classification to information resources that was consistent with the PSM classification system.

Audit findings

2.41 The ANAO found that three entities had incorporated coordination of IT security management into their organisation structure. Agencies where this was assessed as effective had established a security steering committee that comprised IT and business senior management to oversee security issues, thereby providing a mechanism for IT security requirements to be addressed at a senior level.

---

[31] Attorney-General's Department (2005), op. cit., Part C.

2.42 The ANAO found that the majority of audited agencies had taken steps to identify key information resources and define ownership consistent with the government classification requirements. Agencies could, however, further improve existing arrangements and practices by:

- maintaining an information asset register of physical, software and data resources; and
- identifying the information classification of all IT systems that store, process or transmit official information (e.g. electronic mail, calendars and phone books).

3. IT Operational Security Controls

This chapter describes the IT operational security controls used to minimise the risk of harm to agencies' computing services through addressing the objectives of confidentiality, integrity and availability. This chapter discusses the findings of audited agencies against operational security controls.

IT operational security controls

3.1 IT operational security controls are the technologies and processes that enable agencies to protect IT resources, while facilitating electronic communications with external parties. Such controls constitute the range of activities that implement the requirements of an IT security control framework and security policy, and provide confidence that the information security objectives of confidentiality, integrity and availability are being achieved.

3.2 The audit criteria against which the ANAO assessed the adequacy of the audited agencies' IT operational security controls are shown in Table 3.1 below.

Table 3.1

IT operational security controls – audit criteria

IT operational security controls The agency has considered and implemented IT operational security controls to support the organisational objective for the secure management and control of the IT systems. **The components in the scope of this audit, and elements assessed within each of these, are listed below.**		
Component	**Criteria**	**Elements assessed**
Personnel security	Consideration is given to the selection and training of agency personnel.	▪ Security responsibilities ▪ User security awareness training
IT equipment security	Consideration is given to implementing adequate physical and environmental controls to reduce the risk of occurrence of loss, damage or compromise of assets and interruption to business activities.	▪ Security of computing resources ▪ Security of equipment off-site
Network security management	Controls to safeguard information in information systems and protect the supporting network infrastructure are established and documented.	▪ Network security management practices ▪ Security of information exchanges
Logical access management	Controls to prevent and detect unauthorised access to information systems are established and documented.	▪ Access control management ▪ Monitoring system access and use

Source: ANAO

3.3 These components and the respective audit findings are discussed in turn below.

Personnel security

3.4 In reviewing the adequacy of agencies' personnel security controls, the ANAO assessed the extent to which IT security requirements were included in employee job definitions. In addition, the ANAO considered the effectiveness of agencies' user awareness and training arrangements to inform personnel and information resource users of organisational expectations.

Security responsibilities

3.5 Defining security responsibilities within job descriptions is considered to be an effective way of communicating to employees their legal responsibilities and rights. It is also important for agencies to consider specific IT security skill requirements when filling roles that have IT security functions. The ANAO also expected that general responsibilities for establishing and maintaining agencies' security requirements would be reflected in agencies' IT security policies.[32]

User security awareness training

3.6 As discussed in Audit Report No. 41, 2004–05[33], the ANAO has emphasised the importance of a program of security awareness activities to support the establishment and maintenance of a strong security culture. The ANAO has previously recommended that agencies develop a formal plan or strategy for managing and delivering security awareness activities.

3.7 In addition to assessing whether agencies had documented requirements for delivering security awareness activities, the ANAO assessed whether agencies required users to attend IT security induction activities.

Audit findings

3.8 The ANAO found that generally agencies defined security responsibilities within employee job descriptions. In addition, the ANAO found that agencies adequately identified IT security skills for roles that performed specific IT security functions.

3.9 While the majority of agencies audited addressed security requirements either as a part of an employee induction process or through messages or

---

[32] See for example Section 6 Personnel Security, AS/NZS ISO/IEC 17799:2001.

[33] Australian National Audit Office (2005), *Administration of Security Incidents, including the Conduct of Security Investigations*, Audit Report No. 41, 2004–05, p. 30.

posters, entities generally did not document requirements for employee attendance at awareness training.

IT equipment security

3.10 Establishing physical and environmental controls for IT resources that address the PSM requirements of confidentiality, integrity and availability of information resources,[34] reduces the risk of the occurrence of loss, damage or compromise of assets and interruption to business activities.

3.11 The ANAO reviewed the security of computing resources and controls implemented by audited agencies for the purpose of managing the security of computing resources and off-site IT equipment.[35]

Security of computing resources

3.12 Computing resources include physical resources such as buildings, computers and paper documents. These resources may contain sensitive or critical information, or may provide access to resources via a computer network.

3.13 The ANAO assessed the business and system controls established in agencies for protecting their computing resources. The ANAO expected agencies to have established a policy or standard that stated physical and environmental security controls of computing resources. Such processes and practices should also include controls for protecting facilities and equipment and other practices that would help protect the integrity of information systems, such as backup processes, uninterruptible power supplies, environment sensors and equipment protection devices.[36]

Security of equipment off-site

3.14 Flexible working arrangements, such as the ability to work from home, can introduce additional IT security risks that require specific treatment. To address such risks, agencies should establish information security standards for all locations where information equipment connects to an organisation's network. In addition, if applicable to business needs, agencies should develop security policy objectives and procedures for remote working arrangements to

---

[34] Information relating to protecting physical resources is contained in Part E of the PSM and Clause 7 of AS/NZS ISO/IEC 17799:2001. In addition, ACSI 33 provides detailed standards for protecting removable media; servers and communication equipment; server rooms; workstations, physical security incidents; and emergency procedures.

[35] The audit did not assess the suitability of controls such as security perimeters, or physical entry points.

[36] DSD (September 2005), op. cit., Part 1, para. 1.0.23.

ensure that protective measures are consistent with the classification of information stored on the remote IT resource, or accessed by the remote user.

Audit findings

3.15 The ANAO found that, while all agencies displayed a high level of awareness of the need to protect IT equipment, most IT security policy lacked details of the minimum physical and environmental standards needed to protect information assets. The ANAO considers that, in line with business needs, IT equipment security controls would be improved by ensuring agencies' IT security policies clearly define responsibilities and the minimum organisational standards for protecting computing resources.

3.16 The ANAO also found that, generally, agencies had documented and communicated to users, guidance on the use of off-site computing resources and that such guidance included instructions on storing data and protecting information on off-site standalone computers.

Recommendation No.3

3.17 The ANAO recommends that agencies improve IT equipment security practices by ensuring that physical and environmental security controls of computing resources are clearly stated as part of their IT security policy, and that responsibilities for protecting information resources are established and documented[37].

Agencies' responses

3.18 All agencies examined in the audit agreed with the recommendation. Specific comments, which were provided by the Department of Education Science and Training and the Department of Immigration and Multicultural and Indigenous Affairs, are recorded in Appendix 1.

3.19 In addition, the Attorney-General's Department and the Defence Signals Directorate agreed with the recommendation. Additionally, DSD noted that this is a fundamental requirement of ACSI 33.

Network security management

3.20 Network security management encompasses the deployment, maintenance and monitoring of the effectiveness of network security controls to safeguard information in information systems and protect supporting network infrastructure. Network management practices must balance the

[37] The need for a physical security environment and procedures to ensure that equipment that processes security classified information receives an appropriate degree of protection is a minimum standard in the PSM – Attorney-General's Department (2005), op. cit., Part E, para 7.11.

requirement for accessibility of information to both internal and external users, with the requirement to protect information.

3.21 The ANAO assessed the extent to which agencies had implemented network security management practices. In addition, the ANAO reviewed the adequacy of processes for the security of information exchanges through electronic mail and Internet use.

Network security management practices

3.22 Network security management establishes processes for safeguarding information in networks and protecting supporting IT infrastructure[38]. Commonly used network security controls include, deployment of firewalls[39] and implementation of Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS).[40] The ANAO considers that the maintenance of network design and configuration documentation strengthens the effectiveness of the deployment of such controls.

3.23 Effective network security management practices require established and documented procedures that provide instructions for system restart and recovery in the event of system failure, error handling arrangements, as well as housekeeping procedures, such as operational change controls and incident management procedures.[41]

3.24 In addition, where agencies rely on third-party service providers to perform IT services and/or IT security functions, it is important that agencies have contractual arrangements in place to allow, as a minimum, access to network configuration and procedural documentation.

Security of information exchanges

3.25 The ANAO considers that agencies should have a policy in place for use of information exchanges through the Internet and electronic mail and that such a policy should, as a minimum, include:

- guidelines on appropriate use;
- employee responsibilities; and

---

38 AS/NZS ISO/IEC 17799:2001, Clause 8.5.

39 A firewall is a network device that filters incoming and outgoing network data, based on a series of rules (as per ACSI 33 Block 3.10.21).

40 IDSs gather and analyse information from various areas within a network to identify possible security breaches. IPSs protect against threats such as worms and viruses.

41 ACSI 33 contains guidelines for the contents of operating procedures. See DSD (September 2005), ACSI 33, Part 2, Chapter 6.

- plans and procedures to protect the confidentiality and integrity of information during exchanges.

Audit findings

3.26 The ANAO found that, while the majority of agencies had installed firewalls to protect their internal networks from external threats, only two agencies had identified and maintained key IT operational procedures and configuration documentation. In addition, the ANAO found that most agencies did not maintain adequate network design documentation. This was particularly evident of agencies that had contracted to third-party service providers for the provision of IT and/or IT security services.

3.27 The ANAO considers that agencies' IT security practices would be improved by including the maintenance of network documentation as a key responsibility of the IT area. For agencies with outsourced IT services, delivery and maintenance of network documentation should be regarded as a key contractual deliverable and be adequately monitored for performance against the contract requirements.

3.28 The majority of agencies audited had documented electronic mail and Internet usage, but the content did not clearly describe agencies' requirements for monitoring of information exchanges. Half of the agencies audited had deployed detection or prevention controls, such as electronic mail filtering, virus scanning and/or attachment scanning, to assist in managing the security risks associated with electronic mail. However, while these agencies deployed appropriate tools, the ANAO found that only two agencies had documented expectations for deploying network monitoring controls, such as, filtering or monitoring electronic exchanges of information using electronic mail or the Internet. The ANAO considers that this reduces the ability of agencies to assess the effectiveness of system controls in place.

Recommendation No.4

3.29 The ANAO recommends that agencies, as a part of their IT governance arrangements, monitor the effectiveness of network security practices and controls by establishing performance measures and incorporating periodic reporting against these measures.

Agencies' responses

3.30 All agencies examined in the audit agreed with the recommendation. Specific comments, which were provided by the Department of Education Science and Training and the Department of Immigration and Multicultural and Indigenous Affairs, are recorded in Appendix 1.

3.31 In addition, the Attorney-General's Department and the Defence Signals Directorate agreed with the recommendation. Additionally, DSD noted that this is a fundamental requirement of ACSI 33.

Logical access management

3.32 Logical access controls are used to limit access to information systems and information or data by means of appropriate software that requires the identification and authentication of the user. The ANAO considers that effective management of access to agencies' information or data resources requires a clear policy on access to IT systems, supported by processes to uniquely identify and manage all who use them.

3.33 The ANAO reviewed the extent to which the agencies audited had established policies and standards addressing logical access controls.

Access control management

3.34 The ANAO assessed the extent to which agencies had adequately documented and defined business requirements for information system access controls. It was expected that agencies would require users to be uniquely identifiable, state password selection requirements and have a password management policy in accordance with ACSI 33 minimum standards.[42] In addition, it was expected that agencies would have documented and communicated access requirements to information users.

Monitoring system access and use

3.35 The purpose of monitoring access is to detect any deviation from agencies' access control policy and allow for the review of the effectiveness of controls. The ANAO expected that agencies would have established processes and standards for the logging and monitoring of:

- user activity to key systems and applications, for example, those that contain sensitive information;
- the activity of users that have the ability to enable modification or changes to information stored on information resources; and
- unauthorised access attempts.[43]

Findings

3.36 The ANAO found that the majority of agencies had established system access policies that defined agency requirements regarding access to

---

[42] ACSI 33 provides standards and requirements for logical access controls and password selection policy. See DSD (September 2005), op. cit., Part 3, Chapter 6.

[43] AS/NZS ISO/IEC 17799:2001. See for example Clause 9.7.

information systems. Specifically, the ANAO observed that this documentation included guidance regarding the use of passwords, and regular processes to ensure the appropriateness and validity of user access levels across all systems. In addition, the ANAO found agencies' logical access control policies were based on generally accepted standards for password selection.

3.37 The audit also identified that the majority of agencies enabled logging of some key systems. However, this was generally found to be an agency response to a specifically identified requirement, or was implemented at the discretion of the service provider, and not referenced to a specific IT security policy requirement. Seven of the eight agencies lacked documented processes or procedures that included requirements for regular monitoring and review of system access logs. The ANAO considers that this reduced the ability of agencies to monitor and assess the effectiveness of system controls.

3.38 The ANAO considers that agencies' monitoring processes would benefit by taking a risk-based approach to audit logging. Clear specification of standards for audit logging and the inclusion of routine processes for monitoring and reviewing audit logs would enhance management of logical access to information systems.

Recommendation No.5

3.39 The ANAO recommends that agencies, as a part of their system access arrangements, establish standards for the logging of inappropriate or unauthorised activity, and include routine processes for monitoring and reviewing system audit logs.

Agencies' responses

3.40 All agencies examined in the audit agreed with the recommendation. Specific comments, which were provided by the Department of Education Science and Training and the Department of Immigration and Multicultural and Indigenous Affairs, are recorded in Appendix 1.

3.41 In addition, the Attorney-General's Department and the Defence Signals Directorate agreed with the recommendation. Additionally, DSD noted that this is a fundamental requirement of ACSI 33.

Ian McPhee
Auditor-General

Canberra ACT
22 December 2005

Appendices

Appendix 1: Agencies' responses to the audit report

This Appendix contains the general comments received on the audit report, together with any detailed responses to the recommendations that are not shown in the body of the report.

Australian Agency for International Development

The Australian Agency for International Development (AusAID) welcomes and agrees with the recommendations provided in this report.

These recommendations will assist the agency in the ongoing development of its IT Security program.

Australian Office of Financial Management

The Australian Office of Financial Management endorses the recommendations, noting that the report proposes that agencies should assess the benefits of implementing them in light of their own circumstances. The AOFM considers that in making such assessments, agencies should take into account the extent and nature of the risk involved, and the resources required, as well as the processes and controls already in place.

The AOFM will continue to develop its IT security control framework subject to operational and budgetary constraints.

Bureau of Meteorology

Thank you for the opportunity to comment on the ANAO Audit of IT Security Management. The report reminds Australian Government agencies, such as the Bureau of Meteorology, of their obligations and responsibilities to protect the confidentiality, integrity and availability of information systems and the information they hold.

We note that the elements of the audit relevant to the Bureau were conducted in an efficient and professional manner and in doing so minimised possible disruption to our operations. The investigation identified some deficiencies in our IT security management, as well as highlighting areas of good practice, particularly in respect of our mission critical operational weather forecasting systems.

The Bureau of Meteorology supports the Audit's recommendations.

ComSuper

ComSuper agrees with all of the Recommendations contained within this Report and will use this Report, in conjunction with other Reviews and Audits, to guide its IT Security development into the future.

Department of Education, Science and Training

The report draws recommendations from a range of Departments at various level of maturity in IT Security management. As DEST has already established a well structured security control framework for internal DEST information and made substantial progress towards a well structured security control framework for the data network and internet gateway, DEST considers it complies with all the recommendations. It should be noted that DEST's data and internet gateway have been insourced since the audit.

Recommendation No.1

Agreed. DEST currently complies with all aspects of Recommendation 1. DEST's IT security policy is endorsed by the Corporate IT Committee and approved by the Secretary. DEST has a comprehensive set of plans and standard operating procedures within its IT Security section to support the department's operations and governance. These policies, plans and procedures incorporate all requirements of Australian Government policies, standards and guidelines for the safeguarding of information resources. There are clear links between the IT security policy, organisational risk management, and IT security risk assessments.

Recommendation 2.

Agreed. DEST complies with all aspects of Recommendation 2. DEST documents IT security risk assessments, plans and policies. Each year DEST commissions a Threat and Risk Assessment to identify any gaps between DEST's IT environment, DEST business risk requirements, and relevant government policies, standards and guidelines. The follow-up action plan for the following 12 months then addresses any gaps based on risk management principles. In addition, no changes may be made to DEST's IT environment without an assessment against DEST's risk management requirements.

Recommendation 3.

Agreed. DEST complies with all aspects of Recommendation 3. DEST's IT Security policy specifies appropriate security controls of physical and environmental IT resources. DEST has developed standard operating procedures to ensure that the storage, movement or destruction of its IT resources are suitably documented and communicated.

Recommendation 4.

Agreed. DEST has established Internet, network and security automated performance and reporting systems. Ongoing monitoring identifies network availability, intrusion attempts, and compliance with IT security policies at an operating system level. Escalation procedures are detailed in incident response

and investigations plans. DEST IT Security provides periodic statistical reports on these issues to DEST's Audit and Business Assurance Committee.

Recommendation 5.

Agreed. DEST complies with all aspects of Recommendation 5. DEST has systems in place to log inappropriate or unauthorised activity. These systems are monitored proactively and anomalies are pursued through channels identified in DEST's IT Security operational procedures.

Department of the Environment and Heritage

The Department of the Environment and Heritage (DEH) recognises the importance of IT Security Management to its operational activities and statutory responsibilities and agrees with the five recommendations on IT security that are outlined the report.

The Department has already taken actions consistent with the recommendations in a number of areas and is working towards full implementation in others, in accordance with our particular security profile.

Department of Immigration and Multicultural and Indigenous Affairs

The following comments are in response to the five recommendations contained within the audit report of IT Security Management. DIMIA agrees with the findings and recommendations contained within the report and considers itself to be compliant with the intent of the recommendations. DIMIA will strive to further improve its maturity level in relation to the recommendations made.

Recommendation 1

DIMIA has policy in place which combines IT, Personnel and Physical security requirements for the department. DIMIA policy is based on the Australian Government requirements including the Protective Security Manual (PSM) and Australian Government Information Technology Security Manual (*A*CSI 33).

Recommendation 2

DIMIA has a formal risk assessment, acceptance and documentation process that includes Security Risk Assessments, Security Risk Management Plans and System Security Plans. In 2006 DIMIA will continue to improve this model through the introduction of an assurance capability that tracks risk profiles throughout the system lifecycle.

Recommendation 3

DIMIA has security policy in place for maintaining the security of IT equipment. The policy is a joint IT and Protective Security responsibility with clearly defined roles and responsibilities attached to elements of the policy.

Recommendation 4

DIMIA has contract in place with outsourced providers to ensure that network security practices and controls are measured for effectiveness. This includes independent annual reviews of outsourced provider services to obtain assurance that network security is compliant with the Australian Government requirements.

Recommendation 5

DIMIA currently captures extensive system audit logs and has monitoring procedures in place for several systems and platforms. DIMIA will further enhance this capability in 2006 by correlating and reporting on log information.

Department of Transport and Regional Services

The proposed report provides useful and constructive advice and my Department supports all of the reports recommendations.

Attorney-General's Department

The Attorney-General's Department welcomes the report. The report's recommendations are consistent with government policy and represent best practice.

As you are aware the revised Australian Government Protective Security Manual 2005 came into effect on 4 October 2005. We note that the general thrust of Recommendations 1 and 3 of the proposed audit report are currently minimum standards in the PSM.

The Department agrees with the report's recommendations and our comments on of these are included below.

Recommendation 1

Agreed. The need for an IT security policy is currently a PSM minimum standard (Part C, paragraph 4.3)

Recommendation 2

Agreed.

Recommendation 3

Agreed. The need for a physical security environment and procedures to ensure that equipment that processes security classified information receives

an appropriate degree of protection is a minimum standard in the PSM (Part E, para 7.11)

The Protective Security Policy Committee (PSPC), chaired by the Attorney-General's Department, advises the Government on protective security policy issues including the PSM. The PSPC will take into account this recommendation in its review of Part C (Information Security) of the PSM.

Recommendation 4

Agreed.

Recommendation 5

Agreed.

Department of Defence–Defence Signals Directorate

The Defence Signals Directorate (DSD) is pleased to provide this response to the Australian National Audit Office (ANAO) request, to comment upon its proposed report for the audit titled *IT Security Management*.

DSD agrees with the five recommendations in the proposed report and notes they are fundamental requirements of ACSI 33.

The five recommendations are representative of key issues that DSD continues to work with agencies on. Moreover, the notion of ICT security governance that appears throughout the proposed report is a reoccurring theme worthy of much greater awareness throughout the Australian Government.

Appendix 2: Reference to ANAO audits

Protective security audits by the ANAO

Since 1995, the ANAO has conducted a series of audits addressing aspects of protective security as part of its general performance audit program. This series comprises the following reports:

- *Security Preparations for the Sydney Olympics* – Audit Report No. 5, 1998–99;
- *Classification of Information* – Audit Report No. 7, 1999–2000;
- *Internet Security* – Audit Report No. 13, 2001–02;
- *Security Clearances* – Audit Report No. 22, 2001–02;
- *Physical Security* – Audit Report No. 23, 2002–03;
- *Management of Protective Security* – Audit Report No. 55, 2003–04;
- *Administration of Security Incidents, including the Conduct of Security Investigations* – Audit Report No. 41, 2004–05.

Common themes arising from these audits are shortcomings in risk assessments, the completeness and currency of policies and practices surrounding protective security measures, and a lack of rigour with recording and reporting security incidents.

Other relevant ANAO audits

Interim Phase of the Audit of Financial Statements of General Government Sector Agencies for the Year Ending 30 June 2005, Audit Report No. 56, 2004–05.

Appendix 3: Audit objectives and scope

IT security control framework		
The agency has established a framework that reflects management's commitment and attitude to the implementation and maintenance of effective IT security controls and aligns policies, procedures and day-to-day work practices with overall agency objectives for the secure management and control of each part of the IT systems.		
Component	**Criteria**	**Elements assessed**
IT security policy	An IT security policy is documented and provides a high-level IT security policy objective. The policy references existing government policy, standards and guidelines, assigns responsibilities to personnel for the management of IT security, and references other IT security plans or standards.	▪ Policy content ▪ Alignment with IT security risk assessment ▪ Review process
Compliance with internal and external requirements	Relevant criminal and civil law, and statutory, regulatory or contractual obligations, and security requirements are identified and documented.	▪ Compliance with external requirements ▪ Compliance with the Protective Security Manual waiver process ▪ Technical and compliance reviews
IT security organisation structure	An appropriate organisational structure is established to maintain security over information assets.	▪ IT security management structure ▪ Accountability for information resources

IT operational security controls The agency has considered and implemented IT operational security controls to support the organisational objective for the secure management and control of the IT systems.		
Component	**Criteria**	**Elements assessed**
Personnel security	Consideration is given to the selection and training of agency personnel.	▪ Security responsibilities ▪ User security awareness training
IT equipment security	Consideration is given to implementing adequate physical and environmental controls to reduce the risk of occurrence of loss, damage or compromise of assets and interruption to business activities.	▪ Security of computing resources ▪ Security of equipment off-site
Network security management	Controls to safeguard information in information systems and protect the supporting network infrastructure are established and documented.	▪ Network security management practices ▪ Security of information exchanges
Logical access management	Controls to prevent and detect unauthorised access to information systems are established and documented.	▪ Access control management ▪ Monitoring system access and use

Index

R

S

T

U

Series Titles

Audit Report No.22 Performance Audit
Cross Portfolio Audit of Green Office Procurement

Audit Report No.21 Financial Statement Audit
Audit of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2005

Audit Report No.20 Performance Audit
Regulation of Private Health Insurance by the Private Health Insurance Administration Council
Private Health Insurance Administration Council

Audit Report No.19 Performance Audit
Managing for Quarantine Effectiveness–Follow-up
Department of Agriculture, Fisheries and Forestry
Biosecurity Australia

Audit Report No.18 Performance Audit
Customs Compliance Assurance Strategy for International Cargo
Australian Customs Service

Audit Report No.17 Performance Audit
Administration of the Superannuation Lost Members Register
Australian Taxation Office

Audit Report No.16 Performance Audit
The Management and Processing Leave

Audit Report No.15 Performance Audit
Administration of the R&D Start Program
Department of Industry, Tourism and Resources
Industry Research and Development Board

Audit Report No.14 Performance Audit
Administration of the Commonwealth State Territory Disability Agreement
Department of Family and Community Services

Audit Report No.13 Performance Audit
Administration of Goods and Services Tax Compliance in the Large Business Market Segment
Australian Taxation Office

Audit Report No.12 Performance Audit
Review of the Evaluation Methods and Continuous Improvement Processes for Australia's National Counter-Terrorism Coordination Arrangements
Attorney-General's Department
The Department of the Prime Minister and Cabinet

Audit Report No.11 Business Support Process Audit
The Senate Order for Departmental and Agency Contracts (Calendar Year 2004 Compliance)

Audit Report No.10 Performance Audit
Upgrade of the Orion Maritime Patrol Aircraft Fleet
Department of Defence
Defence Materiel Organisation

Audit Report No.9 Performance Audit
Provision of Export Assistance to Rural and Regional Australia through the TradeStart Program
Australian Trade Commission (Austrade)

Audit Report No.8 Performance Audit
Management of the Personnel Management Key Solution (PMKeyS) Implementation Project
Department of Defence

Audit Report No.7 Performance Audit
Regulation by the Office of the Gene Technology Regulator
Office of the Gene Technology Regulator
Department of Health and Ageing

Audit Report No.6 Performance Audit
Implementation of Job Network Employment Services Contract 3
Department of Employment and Workplace Relations

Audit Report No.5 Performance Audit
A Financial Management Framework to support Managers in the Department of Health and Ageing

Audit Report No.4 Performance Audit
Post Sale Management of Privatised Rail Business Contractual Rights and Obligations

Audit Report No.3 Performance Audit
Management of the M113 Armoured Personnel Carrier Upgrade Project
Department of Defence

Audit Report No.2 Performance Audit
Bank Prudential Supervision Follow-up Audit
Australian Prudential Regulation Authority

Audit Report No.1 Performance Audit
Management of Detention Centre Contracts—Part B
Department of Immigration and Multicultural and Indigenous Affairs

Better Practice Guides

Public Sector Audit Committees	Feb 2005
Fraud Control in Australian Government Agencies	Aug 2004
Security and Control Update for SAP R/3	June 2004
AMODEL Illustrative Financial Statements 2004	May 2004
Better Practice in Annual Performance Reporting	Apr 2004
Management of Scientific Research and Development Projects in Commonwealth Agencies	Dec 2003
Public Sector Governance	July 2003
Goods and Services Tax (GST) Administration	May 2003
Managing Parliamentary Workflow	Apr 2003
Building Capability—A framework for managing learning and development in the APS	Apr 2003
Internal Budgeting	Feb 2003
Administration of Grants	May 2002
Performance Information in Portfolio Budget Statements	May 2002
Life-Cycle Costing	Dec 2001
Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	June 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)	June 1999
Commonwealth Agency Energy Management	June 1999
Cash Management	Mar 1999

Security and Control for SAP R/3	Oct 1998
Selecting Suppliers: Managing the Risk	Oct 1998
New Directions in Internal Audit	July 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	July 1997
Management of Corporate Sponsorship	Apr 1997
Telephone Call Centres Handbook	Dec 1996
Paying Accounts	Nov 1996
Asset Management Handbook	June 1996