The Auditor-General
Audit Report No.45 2005–06
Performance Audit

Internet Security in Australian Government Agencies

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 80907 0

Australian National
Audit Office

Canberra ACT
13 June 2006

Dear Mr President
Dear Mr Speaker

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

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

Yours sincerely

Ian McPhee
Auditor-General

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

AUDITING FOR AUSTRALIA

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

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

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

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

http://www.anao.gov.au

Audit Team

Paul Nicoll
John Reid
Melany Kent

Contents

Abbreviations

ACS	Australian Customs Service
ACSI 33	*Australian Government Information and Communications Technology Security Manual*
AFP	Australian Federal Police
ANAO	Australian National Audit Office
ARPANSA	Australian Radiation Protection and Nuclear Safety Agency
DEWR	Department of Employment and Workplace Relations
DSD	Defence Signals Directorate
DITR	Department of Industry, Tourism and Resources
Email	Electronic mail
ICT	Information and Communications Technology
PSM	*Australian Government Protective Security Manual*
USB	Universal Serial Bus

Glossary

availability	Information systems are available and useable when required, and can appropriately resist attacks and recover from failures.
business continuity planning	The objective of business continuity and disaster recovery planning is to ensure the uninterrupted availability of resources to support essential (or critical) business activities.
Australian Government policy and guidelines	Attorney-General's Department's *Australian Government Protective Security Manual* 2005, and the Department of Defence's *Australian Government Information and Communications Technology Security Manual*, March 2005.
confidentiality	Information is observed by, or disclosed to, only those who have a right and need to know.
disaster recovery plan	A plan documenting procedures to recover an ICT processing facility or to recover an operational facility following a disaster.
integrity	Assurance that information has been created, amended or deleted only by the intended authorised means.
Internet	A collection of many computers connected via telecommunication networks throughout the world that communicate through a common language.
ICT security policy	A document that describes the ICT security policies, standards and responsibilities for an agency.
ICT security standard operating procedures	Instructions to all system users, administrators and managers on the procedures required to ensure the secure operation of a system.

ICT system	The hardware and software components of a computer, or computers, used for the communication, storage and processing of information.
risk management plan	A document that identifies risks to the organisation and details appropriate treatments and controls.
server	A computer used to run programmes that provide services to many users.
settings	The way in which a computer is configured for use.
standard operating environment	The way in which a computer is set up for use across an organisation.
system security plan	A document that describes the means for implementing the ICT security policy and risk management plan.
Universal Serial Bus key	A portable device that can be plugged into a computer, which enables computer files to be downloaded for storage, and possible subsequent transfer to other computers.

Summary and Recommendations

Summary and Key Findings

Background

1. It is Australian Government policy that agencies use the Internet to deliver all appropriate programmes and services.[1] This policy aims to improve government services for citizens, and to raise the efficiency and reduce the costs of these services.[2] This policy has led to government agencies significantly increasing the range, volume and complexity of services delivered via the Internet.

2. Some agencies provide public information about the agency and its programmes via a website. Other agencies use the Internet to facilitate transactions between the agency and the business sector or between the agency and individuals, which requires higher levels of protection.

3. While there are many benefits, use of the Internet to provide information and services involves risks for government agencies to manage. These risks have become more acute and electronic attacks more sophisticated over the past few years, and are similar to the risks that private sector companies face in using the Internet in business.

4. Agencies can maintain Internet security by developing and implementing Information and Communications Technology (ICT) policies, plans and procedures that are derived from risk assessments, and which secure and protect their desktop and server computers.

5. The Attorney-General's Department *Australian Government Protective Security Manual* (PSM) 2005 details the minimum standards for the protection of Australian Government information. The PSM states:

> All information systems, whether they are paper based or information and communications technology (ICT) systems, used for the processing, storage or transmission of Australian Government official information require some protection to ensure the system's integrity and reliability. This is because, even when the information processed, stored or transmitted by the system is

---

[1] National Office for the Information Economy, *Better Services, Better Government – The Federal Government's E-government strategy*, Canberra, November 2002, p. iii, available at < www.agimo.gov.au/__data/assets/pdf_file/35503/Better_Services-Better_Gov.pdf>.

[2] Australian Government Information Management Office, *Responsive Government: A New Service Agenda*, Canberra, March 2005, available at <www. agimo.gov.au/publications/2006/march/introduction_to_responsive_government>.

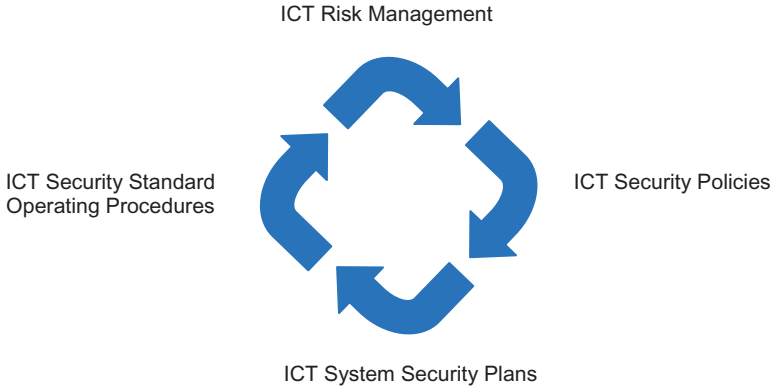
unclassified or authorised for public release, disruption or compromise of the system would prevent or hamper the agency carrying out its functions. The protection for ICT systems should be in accordance with ACSI 33.[3]

6. The PSM is supplemented by the *Australian Government Information and Communications Technology Security Manual* (ACSI 33), which is developed to assist government agencies to achieve an appropriate level of secure information technology. Defence Signals Directorate (DSD) first published the guidelines in 1989. The guidelines include both mandatory requirements and advice. The PSM and ACSI 33 document the Australian Government's protective security policy.

7. ACSI 33 states that agencies must have consistent security risk assessments, policies and plans for their ICT systems. Figure 1 illustrates ACSI 33 requirements of agencies for their ICT security documentation.

Figure 1

ACSI 33 Information and Communications Technology (ICT) security document requirements



Source: ANAO analysis taking into account the requirements of ACSI 33, showing required documentation and linkages between processes.

Note: ICT Risk Management and ICT Security Policies, presented in sequential steps, are developed in parallel.

[3] Attorney-General's Department, *Commonwealth Protective Security Manual 2005*, Canberra 2005, Part C, Principle of effective information security practice, 2.6, C3.

2001 performance audit

8. In 2001, the ANAO completed an audit of *Internet Security within Commonwealth Government Agencies*.[4] The audit concluded that:

> security levels across the audited agencies varied significantly from very good to very poor. For the majority of agency websites in the audit, the current level of Internet security is insufficient, given the threat environment and vulnerabilities identified within a number of agency sites. Further, while some agencies had produced good threat and risk assessments and documentation generally, these were not always effectively administered. Overall, a number of agencies could improve performance in some key areas and all agencies could improve performance in one or more aspects of managing Internet security.

9. Following the 2001 performance audit, the Joint Committee of Public Accounts and Audit held an inquiry into the management and integrity of electronic information within the Australian Government.[5] The Committee made nine recommendations further emphasising the importance of the security and integrity of electronic information within the Australian Government. The Committee's recommendations were for all Australian Government agencies.

2005 *IT Security Management* audit

10. In 2005, the ANAO completed an audit of *IT Security Managemet*.[6] The audit concluded that:

> 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.

11. That audit examined the framework for management and control of ICT security in eight agencies. The ANAO assessed whether the agencies audited had developed and implemented sound ICT security management principles and practices in accordance with the requirements of the PSM and

---

[4] ANAO Audit Report No.13 2001–2002, (2001), *Internet Security within Commonwealth Government Agencies*, ANAO, Canberra, available at <www.anao.gov.au>.

[5] Report 399, *Enquiry into the Management and Integrity of Electronic Information in the Commonwealth,* Joint Committee of Public Accounts and Audit, March 2004, Parliament of Australia, Canberra, available at <http://www.aph.gov.au/house/committee/jpaa/electronic_info/report.htm>.

[6] ANAO Audit Report No. 23 2005-2006, (2005), *IT Security Management*, ANAO, Canberra, available at <www.anao.gov.au>.

ACSI 33. The ANAO made five recommendations for agencies to improve ICT security. Those recommendations are relevant to this report.

Audit objective and scope

12. The audit objective was to form an opinion on the adequacy of a select group of Australian Government agencies' management of Internet security, including following-up on agencies' implementation of recommendations from the ANAO's 2001 audit.

13. The agencies audited were Australian Customs Service (ACS), Australian Federal Police (AFP), Australian Radiation Protection and Nuclear Safety Agency (ARPANSA), Department of Employment and Workplace Relations (DEWR), Department of Industry, Tourism and Resources (DITR) and Medicare Australia. Factors considered in selecting agencies were agency size based on funding levels, whether the agency was included in ANAO's 2001 audit (ACS, ARPANSA, and DEWR), whether the agency's ICT was managed in-house or outsourced, and the nature of the agency's website (that is, general or restricted access).

14. The audit was conducted with the assistance of DSD and involved assessing the management of Internet security through reviewing each agency's ICT:

- compliance with Australian Government minimum policy standards and any agency specific policy;
- business continuity and disaster recovery planning;
- contract management where an agency employed a firm or firms to provide ICT services; and
- desktop and server computer standard operating environments, and email filtering.

15. The audit assessed each agency's ICT security risk assessments and plans, policies and procedures that established the controls for securing an agency's Internet services.

16. The audit also assessed whether ACS, ARPANSA and DEWR had implemented the recommendations from the 2001 audit relating to risk management, installation of security patches, regular review of system event logs, and keeping ICT documentation current.

17. The ANAO did not examine agency networks that communicated national security information.

18. An issues paper was presented to each participating agency. The issues papers assessed each agency's security management framework, risk management, policies, plans and procedures, desktop and server computer standard operating environments, and email filtering. The six issues papers contained 478 suggestions for improvement; 54 relating to ICT risk management, policies and plans, 112 relating to ICT security practices, and 312 relating to desktop and server computer standard operating environments and email filtering.

19. To safeguard the security of the information held by audited agencies, this report does not name agencies or present details of the ANAO's security findings. Rather, the report examines general issues affecting the security of agencies' use of the Internet, and notes any trends observed across agencies.

Overall audit conclusions

20. Since the ANAO 2001 performance audit on Internet security, Australian Government agencies have significantly increased the services delivered by the Internet, while ICT risks from within and outside agencies, and the number and sophistication of electronic attacks have grown rapidly. A major risk to Internet security also comes from within agencies, where personnel have the potential to accidentally or deliberately change information.

21. This environment increases the importance of agencies complying with government policy in the PSM and ACSI 33.

22. Agencies not complying with the PSM and ACSI 33 increase the risks to the confidentiality, integrity and availability of government information, data and systems. Damage may range from embarrassment over website defacement, to unauthorised release of information, and use of a compromised computer to engage in criminal activity.

23. For the six agencies audited, the ANAO concluded that the current level of Internet security was insufficient, given the risks and problems identified through the audit findings. In particular, none of the audited agencies fully complied with the PSM and ACSI 33. This is similar to the conclusion of the ANAO 2001 audit.

24. While the size of the ANAO's sample is relatively small, with ten agencies audited in 2001 and six in 2006, the similarity of the conclusions indicates that all Australian Government entities would benefit from a review of their compliance against the PSM and ACSI 33.

25. A key area in managing Internet security is the administration of new technology, including wireless and voice technologies. Agencies are introducing new technology with the aim of improving productivity and service delivery. Agencies introducing or allowing staff to use new technology within the working environment would benefit from documenting how they balance the risks against the potential benefits. Ordinarily, these would be documented in a business case.

26. The ANAO noted that a number of agencies could improve performance in some key areas, particularly email filtering, and all agencies audited could improve performance in one or more aspects of managing Internet security, such as the development of system security plans.

27. The ANAO has made five recommendations based on the audit findings. Given the need for all agencies to effectively manage their use of the Internet, and the similarity of the conclusion in 2001 with the conclusion in this audit, these recommendations are likely to have relevance to the management and operation of ICT security in all Australian Government agencies.

Key Findings

ICT security management (Chapter 2)

28. For the six agencies audited, the ANAO found that ICT security documentation did not fully comply with the requirements of the PSM and ACSI 33. Non-compliance identified by the ANAO included:

- no systematic and co-ordinated program for the ongoing management of ICT security-related risk assessments;
- security policies and system security plans were not linked to ICT risk assessments and plans; and
- no system security plans.

29. Not adhering to the requirements of the PSM and ACSI 33 increases the potential for agency information to be compromised, affecting the agencies' ability to provide services. These findings are consistent with the recommendations from the 2005 ANAO *IT Security Management* audit report.

30. The ANAO also found that while several of the six agencies had initiated development of business continuity and disaster recovery plans for their Internet services, only one had sound plans in place. The other agencies had deficiencies that included:

- two agencies largely depended upon the knowledge of key staff and had few documented procedures;
- documents were in draft form; and
- some plans had not been regularly reviewed.

31. Lack of appropriate business continuity and disaster recovery planning can increase the time taken to recover information after interruptions to an agency's computer system, and lead to agencies being unable to recover critical Internet services quickly, contributing to a failure to deliver services to the community.

32. The ANAO also concluded that two of the three agencies from the 2001 audit had implemented the recommendations from the audit on risk management and keeping ICT documentation current.

ICT security practices and contract management (Chapter 3)

33. The ANAO found that a majority of the six audited agencies had developed and implemented standard operating procedures that covered Internet security. However, standard operating procedures did not always comply with the requirements of ACSI 33.

34. Key findings of non-compliance identified by the ANAO included:

- inappropriate password management;
- user account privileges inappropriately administered;
- no documented procedures for incident detection and response, management of hardware, and the use of remote access; and
- hardware not adequately secured.

35. Inadequate management of standard operating procedures increases the risk of the misuse or theft of information, infection of computer systems by malicious code, and use of computer systems to commit fraud.

36. The ANAO also found that there were particular weaknesses in the management of new technology. For example:

- policy development and supporting procedures for the introduction of new technology, such as USB keys, was generally poor. Where it existed, compliance within agencies was also often poor;
- personnel in one agency were found to be using USB keys to move data from one system to another without documented controls; and
- one agency had developed procedures for procuring USB keys. These procedures were not based on a risk assessment and, accordingly, were incomplete.

37. When introducing new technology like USB keys, the ANAO also found limited evidence that the agencies were balancing risks against the benefits afforded by new technology. Ordinarily, these would be documented in a business case.

38. Agencies in managing new technology should conduct risk assessments and develop and implement policies, plans and procedures for their use, and better manage risks to their business.

39. Four agencies had outsourced their ICT services, and contracts for two of these agencies were poorly drafted and managed. The ANAO identified several weaknesses, including contracts that:

- contained unclear statements on responsibility for development of ICT documentation and procedures;
- contained insufficient detail to adequately monitor performance;
- did not clearly detail what service provider information the agency has the right to review;
- did not provide the agency with full access to the contractor's documentation on the security of the agency's information; and
- allowed inadequate reporting by service providers.

40. One of the three agencies from the 2001 audit had implemented the recommendation from the audit on regularly reviewing event logs.

ANAO testing of ICT security (Chapter 4)

41. For the six agencies audited, the ANAO found that the technical security of each agency's web server[7] was adequate. However, all the agencies could improve the security of their desktop computer[8] standard operating environments, and improve their email filtering.

42. Weaknesses identified in the desktop computer standard operating environment included:

- inappropriate access controls, such as users with more access rights than required for their work;
- agency personnel able to download information of their choice from the Internet;
- inadequate auditing of system event logs, including logs that did not record and hold sufficient information for auditing of security events; and
- inappropriate levels of system patching.

43. As part of the audit methodology, emails were sent to auditee agencies to test whether they bypassed email filters, highlighting any deficiencies in the agencies' email filtering policies or applications. The ANAO found that email filtering in all six agencies was inadequate.

Agencies' responses

44. The six agencies examined in the audit agreed with the recommendations.

---

[7] A web server is a computer that manages and shares web based programmes and services accessible from computers connected to the Internet.

[8] A desktop computer is a computer other than a server that is used on a desk in an office or home.

Recommendations

Although the following recommendations are based on the findings of fieldwork at the six audited agencies, they are likely to be relevant to all entities in the Australian Government. Therefore, there would be benefits in all entities assessing 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.

Recommendation No.1
Para 2.23

The ANAO recommends that agencies include coverage of their Internet services in their business continuity and disaster recovery plans.

Recommendation No.2
Para 3.30

The ANAO recommends that agencies develop business cases for introducing new technology, and include how they balance potential benefits against potential risks.

Recommendation No.3
Para 3.57

The ANAO recommends that agency Information and Communications Technology contracts include:

(a) requirements for contractors to comply with Australian Government security policies, as defined in the Attorney-General's Department's and the Defence Signals Directorate's policy documentation;

(b) agency's requirements for security reporting;

(c) a statement as to who is responsible for developing and maintaining Information and Communications Technology security plans and procedures; and

(d) reporting and performance measurement requirements.

Recommendation No.4
Para 4.41

The ANAO recommends that agencies review their compliance with the *Australian Government Protective Security Manual* and the *Australian Government Information and Communications Technology Security Manual*.

Recommendation No.5
Para 4.53

The ANAO recommends that agencies develop and implement policies that permit them to block potentially malicious emails.

Agencies' responses to the recommendations

45. Each of the six agencies audited agreed with the recommendations.

Audit Findings and Conclusions

1. Introduction

This chapter is a brief background to the audit. It provides information on why government agencies use the Internet to deliver programmes and services, and the risks they must manage in using the Internet. It also sets out the audit objective and criteria, scope, methodology, and the structure of the report.

Background

1.1 It is Australian Government policy that agencies use the Internet to deliver all appropriate programmes and services.[9] This policy aims to improve government services for citizens, and to raise the efficiency and reduce the costs of these services.[10] This has led to government agencies significantly increasing the range, volume and complexity of services delivered via the Internet.[11] The most recent information available on Australian Government expenditure on Information and Communications Technology (ICT) is for 2002–03. In that year, the government spent an estimated $4.2 billion.[12]

1.2 In 2001–02 the ANAO, in conjunction with the Department of Defence's Defence Signals Directorate (DSD), conducted an audit of *Internet Security within Commonwealth Government Agencies* (2001 audit).[13] The audit concluded:

> security levels across the audited agencies varied significantly from very good to very poor. For the majority of agency websites in the audit, the current level of Internet security is insufficient, given the threat environment and vulnerabilities identified within a number of agency sites. Further, while some agencies had produced good threat and risk assessments and documentation generally, these were not always effectively administered. Overall, a number of agencies could improve performance in some key areas and all agencies

---

9 National Office for the Information Economy, *Better Services, Better Government – The Federal Government's E-government strategy*, Canberra, November 2002, p. iii, available at < www.agimo.gov.au/__data/assets/pdf_file/35503/Better_Services-Better_Gov.pdf>.

10 Australian Government Information Management Office, *Responsive Government: A New Service Agenda*, Canberra, March 2005, p. 3, available at <www. agimo.gov.au/publications/2006/march/introduction_to_responsive_government>.

11 The Internet is a collection of many computers connected via telecommunication networks throughout the world that communicate through a common language. *Managing internet security, Good Practice Guide, Auditor General Victoria, June 2004*, available at <www.audit.vic.gov.au>.

12 ANAO Audit Report No.56 2004–2005, (2005), *Interim Phase of the Audit of Financial Statements of General Government Sector Entities for the Year Ending 30 June 2005*, ANAO, Canberra, p. 18, available at <www.anao.gov.au>.

13 ANAO Audit Report No.13 2001–2002, (2001), *Internet Security within Commonwealth Government Agencies*, ANAO, Canberra, available at <www.anao.gov.au>.

could improve performance in one or more aspects of managing Internet security.

1.3 The 2001 ANAO performance audit made seven recommendations:

- agencies should adopt a structured approach to the management of Internet security, employing a sound risk management model;
- agencies should ensure that appropriate risk assessments are conducted;
- agencies should avoid default installations of operating system and web server software;
- agencies should test and install security patches in a timely manner;
- security administrators should regularly review system event logs;[14]
- agencies should ensure that applications which support transactions with users, such as active content,[15] are reviewed for secure coding practices; and
- agencies should ensure that relevant documentation is kept up-to-date.

1.4 Following this audit, the Joint Committee of Public Accounts and Audit held an inquiry into the management and integrity of electronic information within the Australian Government.[16] The Committee made nine recommendations further emphasising the importance of the security and integrity of electronic information within the Australian Government. The Committee's recommendations were for all Australian Government agencies.

1.5 The ICT environment has changed since these reports were completed, and agencies have significantly increased their use of the Internet to deliver information and services. This has resulted in additional opportunities for better service delivery by Australian Government agencies, as well as increased risks to the confidentiality, integrity and availability of government information, data, and systems.

---

[14] A log is a file that lists certain events that have occurred. For example, a log might list each time a person tries to log on to a computer network and fails.

[15] Active content refers to a web based application (a piece of software stored on the web server) which responds to user input, for example, providing access to a database, access to another application on the web server, or generating an email message.

[16] Report 399, *Inquiry into the Management and Integrity of Electronic Information in the Commonwealth,* Joint Committee of Public Accounts and Audit, March 2004, Parliament of Australia, Canberra, available at <http://www.aph.gov.au/house/committee/jpaa/electronic_info/report.htm>.

Internet security

1.6 ICT security is concerned with the security of electronic systems, including computers, voice and data networks. Internet security is a subset of information technology security. Effective management of Internet security requires Australian Government agencies to have well-developed, coordinated, and implemented ICT security policy, plans and standard operating procedures, underpinned by a secure desktop and server computer standard operating environment.

1.7 The Internet can be used in a variety of ways, for example:

- browsing the World Wide Web from a desktop computer;
- using the Internet to send and receive emails;
- presenting public information about the agency through a website accessible to all; and
- receiving and providing information over an Internet connection.

1.8 Agencies using the Internet to provide information and services are faced with a range of risks that must be managed to ensure the confidentiality, integrity and availability of Australian Government information.

Internet security risks

1.9 Risks to the security of government agency websites have become more acute over the past few years. These risks area similar to the risks that private sector companies face in using the Internet in business. For Australian Government agencies to maintain Internet security, they need to continue to develop, improve, and review their ICT security management.

1.10 Internet security risks come from inside and outside government agencies, with the main threats to agencies using the Internet being:

- infection of information and systems by malicious code;[17]
- use or alteration of information and systems by unauthorised users;[18]

---

[17] Malicious code is software designed to damage data, steal information or compromise the ability to use a computer. Department of Communications, Information Technology and the Arts, *Internet Security Essentials For Small Businesses*, Australian Government, 2005, Canberra, p. 11, available at <www.dcita.gov.au/e-security>.

[18] Unauthorised access is where a person who has not been given permission to access information does so.

- limitations to information and systems by denial-of-service attacks;[19]
- defacement of agency websites;[20] and
- malicious or accidental insider attack.

1.11 Failure to manage these risks can have wide-ranging consequences for agencies and their performance, including:

- a deterioration of the agency's reputation;
- reduced public confidence in the agency's online services;
- unauthorised disclosure or alteration of confidential data;
- unauthorised disclosure of clients' personal details;
- financial loss through online fraud; and
- not having information and/or systems available for use.[21]

1.12 DSD manages the recording of security incidents in Australian Government agencies through its *Information Security Incident Detection, Reporting and Analysis Scheme*. The Scheme has four categories of ICT security incidents, with DSD recommending that agencies report to them on more notable or serious matters.[22] Agencies can decide not to report incidents provided they first consult with DSD, and the latter approves.

1.13 Internet related security incidents occur for several reasons. Computer hackers attempt to exploit vulnerabilities in computer operating systems, for example, to gain unauthorised access to information and to control those systems. Some hackers operate without malicious intent, breaking into computer systems to satisfy their curiosity or to test their technical skills. Others breach computer systems with malicious or criminal intent, and can inflict significant damage. Damage may range from embarrassment over website defacement, to compromised or unauthorised release of information and use of a compromised computer in perpetrating crimes.

---

[19] A denial-of-service attack is where a server is flooded with service requests until it is overloaded, at which time it slows down and/or crashes. When that occurs, the government agency cannot use the Internet to deliver its services.

[20] Defacement of an agency's website occurs when a page on a website, usually the Home Page, is replaced with different text and/or images. Defacement may cause the agency embarrassment and damage its image.

[21] *Managing internet security, Good Practice Guide*, Auditor General Victoria, June 2004, available at <www.audit.vic.gov.au>.

[22] DSD requires agencies to rank the more notable or serious security incidents as Category 3 or Category 4. For further information, refer to <www.aisep.gov.au/infosec/assistance_services/incident.html>.

1.14 Security incidents also occur from within government agencies. For example, staff using email to correspond with other agencies or businesses, can unknowingly introduce malicious code through opening email attachments.

1.15 Table 1.1 shows the number of security incidents that Australian Government agencies reported to DSD from 2001–02 to 2004–05. Over this period there was a 129 per cent increase in the number of Internet security incidents Australian Government agencies reported to DSD.

Table 1.1

Australian Government agencies' reporting of Internet security incidents to DSD, 2001–02 to 2004–05

Security incidents	2001–02	2002–03	2003–04	2004–05	Total
Category 1 incidents (minor)					
Email scams[23]	0	1	1	3	**5**
Category 2 incidents					
Attempted unauthorised access	3	0	16	41	**60**
Attempted denial-of-service attack	2	5	1	0	**8**
Virus infection	19	11	23	12	**65**
Category 3 incidents					
Unauthorised access	5	9	10	1	**25**
Website defacement	2	5	10	7	**24**
Denial-of-service attack	0	14	1	3	**18**
Virus infection	0	0	5	4	**9**
Category 4 incidents (major)					
Virus infection	0	0	3	0	**3**
Total	**31**	**45**	**70**	**71**	**217**

Source: DSD data provided December 2005.

1.16 DSD advised the ANAO that the data in Table 1.1 under-represents government Internet security incidents due to agencies under-reporting.

1.17 In addition, the results of the *Australian Computer Crime and Security Survey 2005*,[24] showed:

- electronic attacks were sourced both externally and internally;

[23] Email scams are an attempt to sell products or services via email where such goods or services do not exist.

[24] The Australian High Tech Crime Centre, Australian Federal Police, New South Wales Police, Northern Territory Police, Queensland Police, South Australian Police, Tasmanian Police, Victorian Police, Western Australian Police and AusCERT worked together to produce the *2005 Australian Computer Crime and Security Survey*. The survey represents trends and issues that Australia's public and private sector organisations face in computer crime and network security.

- infections from viruses were the most common form of electronic attack reported; and
- the scale and sophistication of viruses used to support identity theft was increasing.

1.18 In a recent speech, the Attorney-General stated that:

> I saw a figure recently that worldwide damage from Internet worms such as Bagle, Nesky and Mydoom is estimated to have exceeded $100 billion, and of course this impact does not discriminate between government, business and the community. [25]

1.19 To counter these threats, government agencies are continuously improving their Internet security. However, agency websites are still being defaced, accessed illegally, and infected with viruses. Such interference with government agency websites can reduce agency clients' access to government services, such as employment and health services, and information about educational institutions.

1.20 Agencies can better manage these risks through developing, implementing and maintaining ICT security policies, plans and standard operating procedures derived from a sound ICT risk management approach.

Australian Government protective security policy and guidelines

1.21 The Attorney-General's Department *Australian Government Protective Security Manual* (PSM) 2005 is the Australian Government's protective security policy. The PSM, first published in January 1991, details the minimum standards for the protection of Australian Government information that agencies must meet in their operations. The PSM states:

> All information systems, whether they are paper based or information and communications technology (ICT) systems, used for the processing, storage or transmission of Australian Government official information require some protection to ensure the system's integrity and reliability. This is because, even when the information processed, stored or transmitted by the system is unclassified or authorised for public release, disruption or compromise of the system would prevent or hamper the agency carrying out its functions. The protection for ICT systems should be in accordance with ACSI 33.[26]

---

[25] Lunch address, Annual Seminar, Information Security Interest Group, 25 November 2005, available at <www.ag.gov.au/agd/WWW/agdhome.nsf/Page/Latest_News>.

[26] Attorney-General's Department, *Commonwealth Protective Security Manual 2005*, Canberra 2005, Part C, Principle of effective information security practice, 2.6, C3.

1.22 The PSM is supplemented by the *Australian Government Information and Communications Technology Security Manual* (ACSI 33) March 2005, which is designed to enable government agencies to achieve an appropriate level of secure information technology. DSD first published the guidelines in 1989. The guidelines include both mandatory requirements and advice.

1.23 Agencies deviating from a mandatory statement[27] must seek from DSD a waiver in accordance with the requirements of the PSM. Agencies deviating from presumptively mandatory statement[28], must document their decision process, assess residual risk, set a date for a review of the decision and get management approval.

Audit approach

Audit objective and criteria

1.24 The objective of the audit was to form an opinion on the adequacy of a select group of Australian Government agencies' management of Internet security, including following-up on agencies' implementation of the recommendations from the previous audit.[29]

1.25 The audit criteria involved assessing the management of Internet security through reviewing each agency's ICT:

- compliance with Australian Government minimum policy standards and agency specific policy;
- business continuity and disaster recovery planning;
- contract management where an agency employs a firm or firms to provide ICT services;
- desktop and server computer standard operating environments; and
- email filtering.

1.26 The audit assessed each agency's ICT security risk assessments and plans, policies and procedures that established the controls for securing an agency's Internet services.

---

[27] A must or must not statement.

[28] A should or should not statement.

[29] Op. cit., ANAO Audit Report No. 13 2001–2002.

DSD assistance

1.27 The ANAO conducted this audit with expert assistance from DSD.[30] DSD staff were appointed under provisions of the *Auditor-General Act 1997* for the purpose of this audit. The role of the DSD team was to provide specialist knowledge for assessing each agency's ICT security planning and operational procedures, and to assess elements of each agency's Internet services.

Audit scope

1.28 The focus of this audit was management of Internet security. The agencies audited were selected on the basis of:

- agency size (as measured by its funding levels);
- whether or not the agency was included in the 2001 audit;
- whether the agency's ICT was managed in-house or outsourced; and
- the nature of the agency's Internet presence (that is, general or restricted access).[31]

1.29 Table 1.2 lists the six agencies audited and provides detail on criteria used to select the agencies.

---

[30] By government directive in October 1986, DSD was designated as the national computer and communications security authority, and ascribed particular roles in providing advice and assistance to Australian Government departments and agencies.

[31] General Internet access allows the public to view information about an agency and its products or services.

Restricted Internet access requires prospective users to identify themselves before they can receive or provide information, or access another kind of service.

Table 1.2

Agency selection criteria details

Agency	Appropriation[32]	2001 audit	ICT management	General / restricted Internet access
Australian Customs Service (ACS)	$783 million[1]	Yes	Outsourced	General
Australian Federal Police (AFP)	$860 million[2]	No	Part Outsourced	General
Australian Radiation Protection and Nuclear Safety Agency (ARPANSA)	$11 million[3]	Yes	In-house	General
Department of Employment and Workplace Relations (DEWR)	$24.3 billion[4]	Yes	In-house	General and Restricted
Department of Industry, Tourism and Resources (DITR)	$1.2 billion[5]	No	Outsourced	General
Medicare Australia[33]	$24 billion[6]	No	Outsourced	General and Restricted

Source: ANAO analysis.

Note: ACS, ARPANSA and DEWR were included in the 2001 ANAO performance audit.

1.30 The ANAO did not examine any agency networks that communicated national security information. Also, the ANAO only examined a sample of Internet services, and did not include coverage of wireless or voice technologies related to use of the Internet.

Internet services examined

1.31 The ANAO examined a desktop and web server computer standard operating environment in each agency. These computers were selected for examination as they are both used extensively in Internet activities. These

---

[32] Note 1: Portfolio Budget Statements 2005–06, Attorney-General's Portfolio, Australian Customs Service Total Appropriations 2005–06, Outcome 1, p. 105.

Note 2: Portfolio Budget Statements 2005–06, Attorney-General's Portfolio, Australian Federal Police, Total Appropriations 2005–06, Outcome 1 and 2, p. 142.

Note 3: Portfolio Budget Statements 2005–06, Health and Ageing Portfolio, Australian Radiation Protection and Nuclear Safety Agency, Total Appropriations, p. 230.

Note 4: Portfolio Budget Statements 2005–06, Employment and Workplace Relations Portfolio, Department Employment and Workplace Relations, Total Administered Appropriations, Outcome 1, 2 and 3, p. 20.

Note 5: Portfolio Budget Statements 2005–06, Industry, Tourism and Resources Portfolio, Department of Industry, Tourism and Resources, Total Administered Appropriations, Outcome 1 and 2, p. 22.

Note 6: Portfolio Budget Statements 2005–2006 Health and Ageing Portfolio, Department of Health and Ageing, Administered Appropriations, Outcome 2, p.75.

[33] Prior to 1 October 2005, Medicare Australian was the Health Insurance Commission.

computers can be damaged from within or outside an agency, and if not appropriately secured can lead to agency information and/or services being disrupted. A brief description of the web server tested in each agency is outlined below.

Table 1.3

Web servers tested in each agency

Agency	Web servers tested in each agency
ACS	The web server that hosts ACS's website <http://www.customs.gov.au>. This web server provides ACS Media Releases and other general public information about ACS.
AFP	The web server that hosts the AFP website <http://www.afp.gov.au> and <http://www.ahtcc.gov.au>. This web server provides public information about the AFP and the Australian High Tech Crime Centre.
ARPANSA	The web server that hosts ARPANSA's website <http://www.arpansa.gov.au>. This web server provides public information about ARPANSA's services, media releases and issues of public concern.
DEWR	The server that hosts some of DEWR's critical web applications. This web server provides a restricted Internet connection, therefore no website address is provided. The web server examined supports the Job Network and the Australian Job Search applications. This web server, which is connected to other servers, manages millions of transactions per day.
DITR	The server that will host DITR's updated website, <http://www.industry.gov.au>. This web server provides general public information about DITR.
Medicare Australia	The web server that hosts components of the Medicare Australia Online Bulk Billing system. This web server provides a restricted Internet connection, therefore no website address is provided. The Medicare Australia Online Bulk billing system provided for approximately 2.7 million claims in 2004–05, with payments of approximately $5.8 billion.

Source: ANAO analysis.

Audit methodology

1.32 The audit involved:

- interviewing each agency's ICT security staff;
- reviewing ICT security planning documentation;
- reviewing elements of contract management; and
- testing and analysing agencies' desktop and server computer standard operating environments and email filtering.

1.33 The audit assessed each agency's ICT risk assessments, policies, plans and procedures as they establish the controls and set out the procedures on which the agency's Internet services were based.

1.34 This audit follows the ANAO's recent audit report on *IT Security Management*.[34] That audit examined the management and control of ICT security in eight agencies. The report assessed whether those agencies had developed and implemented sound ICT security management principles and practices in accordance with the PSM and ACSI 33. The report made five recommendations for agencies to improve their ICT security. Those recommendations are relevant to this report.

1.35 Government agencies have significantly increased the range, volume and complexity of services delivered via the Internet over the past five years. This increase in Internet use has been accompanied by an increase in associated risks and the number and sophistication of attacks. The ANAO has conducted several performance audits related to agencies' use of the Internet since 2001 as the Internet has become increasing important in delivering services by agencies. These are listed in Appendix 1.

1.36 Fieldwork for this audit was conducted from June to October 2005, in Canberra, Sydney, Melbourne and Adelaide.

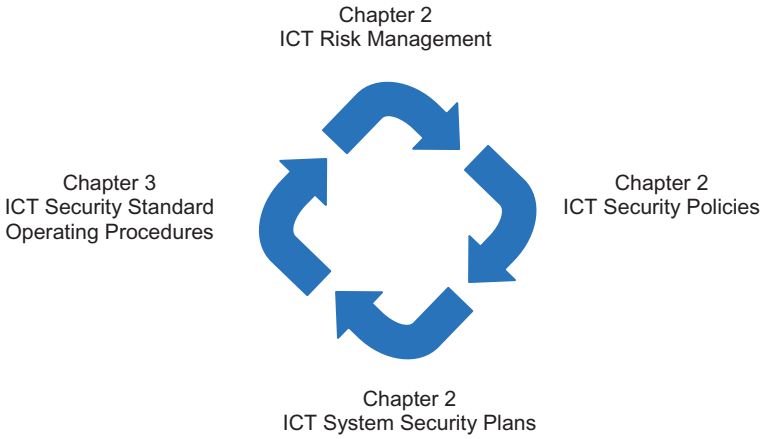
1.37 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of $378 000.

Structure of this report

1.38 This audit report has four chapters. Chapters 2 and 3 discuss ICT security management, and ICT security practices and contract management. Figure 1.1 shows the documentation cycle for ICT security and how it relates to Chapters 2 and 3.

[34] ANAO Audit Report No. 23 2005–06, (2005), *IT Security Management*, ANAO, Canberra, available at <www.anao.gov.au>.

Figure 1.1
ACSI 33 Information and Communications Technology security document requirements



Source: ANAO analysis taking into account the requirements of ACSI 33.

1.39 Chapter 4 examines the results of assessments of agencies' desktop and server computer standard operating environments, and email filtering.

2. ICT Security Management

This chapter examines ICT security management including risk assessments and plans, security policies, system security plans and business continuity and disaster recovery plans in ACS, AFP, ARPANSA, DEWR, DITR and Medicare Australia.

Introduction

2.1 ICT security requires well-developed and implemented risk assessments and plans, security policies and system security plans. The Attorney-General's Department's *Australian Government Protective Security Manual* (PSM) and the Defence Signals Directorate's ACSI 33 provide agencies with the minimum standards essential in the development and implementation of these documents.

2.2 ICT security also requires agencies to develop and maintain business continuity and disaster recovery plans.[35] Business continuity and disaster recovery plans should be regularly reviewed and tested, so that they remain relevant to the organisation's operational environments and business risks.

2.3 The ANAO reviewed ICT risk assessments, policies and plans against the PSM and ACSI 33 requirements and sound practice for each of the six agencies in this ANAO sample. The ANAO also examined whether three of the agencies audited in the ANAO 2001 audit (ACS, ARPANSA and DEWR) had implemented the recommendations on risk management and on keeping ICT security documentation up-to-date. Across the six agencies, the ANAO issues papers made 54 suggestions for improvements to agencies documentation and implementation of their ICT security management.

[35] Business continuity planning outlines the organisation's preferred approach to dealing with disruptions to key business processes. The key documents that generally comprise the business continuity plan include the: business group (or service area) recovery plans; disaster recovery plans; emergency response and evacuation procedures; backup and recovery procedures; and communication and media liaison strategies. Collectively, these documents detail information critical to determining the: declaration point of a disaster; immediate response procedures; minimum level of resources necessary to support a degraded level of service from the key business processes; method of operation in the interim period (between disaster declaration and the restoration of normal operations); and disaster recovery procedures necessary to restore or recover lost business functions. ANAO Audit Report No.53, 2002–2003, (2003), *Business Continuity Management Follow-on Audit*, available at <www.anao.gov.au>.

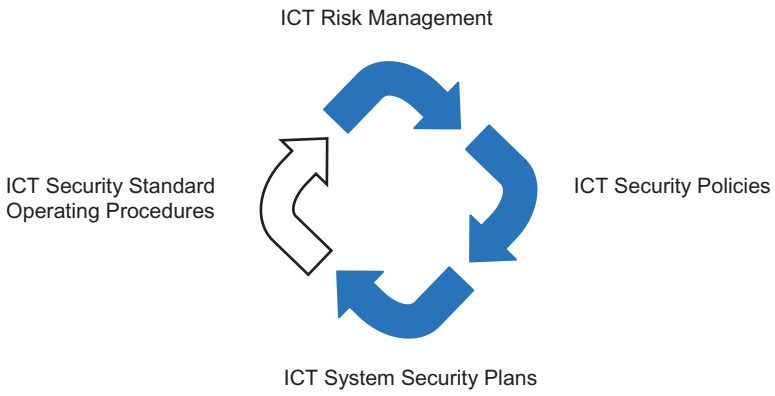
ICT security planning

2.4 ICT systems that process, store or communicate official information must comply with the Attorney-General's Department's PSM requirements. The PSM advises that protection for ICT systems should be in accordance with ACSI 33.

2.5 Figure 2.1 illustrates ACSI 33 requirements to agencies on ICT security documentation. The blue arrows represent the documents examined in this chapter. ACSI 33 requires that agencies' ICT security documents be consistent with each other and with agencies' other security documents.[36]

Figure 2.1

ACSI 33 Information and Communications Technology security document requirements



Source: ANAO analysis taking into account the requirements of ACSI 33.

Note: ICT Risk Management and ICT Security Policies are developed in parallel.

Risk management

2.6 Agencies using the Internet to provide information and/or services are increasingly faced with more sophisticated electronic attacks. These attacks heighten the need for agencies to keep under review their risk assessments and risk management plans. In addition, these attacks increase the importance of agencies developing approaches to mitigate their key business risks, taking account of the information and kinds of services each agency provides to the community.

[36] ACSI 33, 2.2.4 to 2.2.8.

2.7 The PSM states that agencies must ensure all information for which they are responsible is secured. Agencies must have procedures to identify risks, and must devise and implement cost effective measures to reduce risks to acceptable levels. Also, agencies should conduct risk assessments for their ICT systems, and have risk management plans to address those risks.[37] ACSI 33 states that agencies should ensure that every system is covered by a risk management plan. For the six agencies in the ANAO's sample, the ANAO assessed their ICT risk management against the requirements of the PSM and ACSI 33.

2.8 The ANAO found that three agencies had current risk assessments that included analysis of risks to their ICT services, including those services delivered through the Internet. The ANAO also found that some agencies' risk assessments and plans:

- had not been updated for up to four years; or
- were in draft form; and/or
- were not linked to their security planning documentation.

2.9 Agencies that do not maintain their risk management documentation will not have an accurate picture of their security environment and associated business risks. These agencies would be less able to establish and maintain effective ICT security controls, as they would not have a comprehensive view of risks to their businesses.

2.10 For agencies to effectively manage their ICT security risks, they need to examine and document them, and develop and implement approaches to mitigate those risks. Expenditure on protection measures needs to be cost-effective, and in some cases the merits of using particular devices should also be assessed.

ICT security policy

2.11 ICT security policies describe how an agency protects its ICT resources, and allows management to direct and commit to ICT security. ACSI 33 states that agencies must have an ICT security policy document,[38] and that this document be approved by the security executive, senior executive manager or

[37] ACSI 33, 2.2.4 to 2.2.7.

[38] ACSI 33, 2.2.5.

agency head, contain a schedule for review at regular intervals, and be security classified.

2.12 For each of the six agencies in the ANAO's sample, the ANAO evaluated whether a clear link existed between the agencies' ICT security policy requirements and the contents of risk assessments, and whether their security policy complied with the requirements of the PSM and ACSI 33.

2.13 The ANAO found that all agencies had developed an ICT security policy. However, four agencies' ICT security policies were not clearly linked to the agencies' risk assessments. Also, some agencies' ICT security policy did not comply with the PSM and ACSI 33 requirements, as they were not appropriately classified and did not contain a schedule for reviewing the documents at regular intervals in response to events such as major system changes.

2.14 ICT security policy developed without consideration of ICT risk assessments weakens an agency's ability to develop appropriate ICT security controls.

ICT system security plans

2.15 The purpose of a system security plan is to indicate how an agency will address matters for individual computer systems, identified in its security policy and risk management plan. ACSI 33 states that agencies should have a system security plan for each ICT system.

2.16 Five agencies audited did not have system security plans. The absence of system security plans means the agencies were not adequately:

- documenting how to implement security requirements identified in the ICT security policy and risk management plan for particular ICT systems; and
- implementing appropriate controls.

2.17 Agencies that have system security plans are better able to implement the agency's security requirements for their ICT systems than agencies that do not have system security plans.

Business continuity and disaster recovery planning

2.18 The objective of business continuity and disaster recovery planning is to ensure the uninterrupted availability of resources to support essential (or critical) business activities.[39]

2.19 The ANAO addressed business continuity in its *Audits of the Financial Statement of Australian Government Entities for the Period Ended 30 June 2005.* That audit report stated:

> an important aspect of an entity's governance and risk management strategies is an assessment of the risk to the continued availability of service delivery and information. A number of entities still have work to perform to ensure they have developed, implemented, tested and documented comprehensive business continuity plans.[40]

2.20 The ANAO examined ICT business continuity and disaster recovery plans for each of the six agencies in its sample, and found that one agency had a sound business continuity and disaster recovery planning process. The other agencies had deficiencies that included:

- two agencies largely depended upon the knowledge of key staff and had few documented procedures;
- documents were in draft form; and
- some plans had not been regularly reviewed.

2.21 Lack of appropriate business continuity and disaster recovery planning can increase the time taken to recover information after interruptions to an agency's computer system, and lead to agencies being unable to recover critical Internet services quickly, contributing to a failure to deliver services to the community.

2.22 Lack of planning can also lead to Internet services being compromised and information lost, reducing the agency's effectiveness and harming its reputation. These problems increase the agency's and its clients' costs where the agency cannot recover critical functions and data.

---

[39] Op. cit., Business continuity planning.

[40] ANAO audit report No. 21 2005-06, (2005), *Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2005* , ANAO, Canberra, p.59, available at <www.anao.gov.au>.

Recommendation No.1

2.23 The ANAO recommends that agencies include coverage of their Internet services in their business continuity and disaster recovery plans.

Australian Customs Service response

2.24 Agreed.

Australian Federal Police response

2.25 Agreed.

Australian Radiation Protection and Nuclear Safety Agency response

2.26 Agreed.

Department of Employment and Workplace Relations response

2.27 Agreed. Internet services are a key component of DEWR's business continuity and disaster recover plans.

Department of Industry, Tourism and Resources response

2.28 Agreed. DITR agrees with the recommendation. DITR is taking steps in 2006-07 to both document the coverage of Internet services within business continuity and disaster recovery plans and to provide a technical solution to maintaining its Internet services.

Medicare Australia response

2.29 Agreed**.** Business Continuity and Disaster Recovery are run as half yearly cycled projects within the agency. Internet services are included to ensure end to end business continuity especially for ebusiness services. These ongoing projects, report to the Executive Officer in charge of Information Technology services.

Implementation of 2001 audit recommendations

2.30 The ANAO examined if ACS, ARPANSA and DEWR - agencies audited in the ANAO 2001 audit, and again in this audit - had implemented the recommendations from the ANAO 2001 audit on risk management and keeping relevant security documentation up-to-date.

2.31 The ANAO found:

- two agencies had appropriate risk management for their Internet services;
- all had updated their security policies;
- one agency had current system security plans; and
- all were in the process of updating their business continuity or disaster recovery plans.

2.32 Overall, the ANAO concluded that two of the agencies had generally improved their management of Internet security.

3. ICT Security Practices and Contract Management

This chapter examines several security standard operating procedures in ACS, AFP, ARPANSA, DEWR, DITR and Medicare Australia. Within this sample, it also examines contract management in those agencies that employ a firm or firms to provide ICT services.

Introduction

3.1 A key component of Internet security is preparation and implementation of security standard operating procedures. The primary function of security standard operating procedures is to ensure implementation of and compliance with the agency's security plans. ACSI 33 states that these procedures are instructions to all system users, administrators and managers on how to ensure the secure operation of computer systems.[41]

3.2 This chapter examines the standard operating procedures for securing each of the following aspects of agency Internet use: access control, auditing system event logs, change management, incident detection and response, hardware security, introducing and using new technology, remote access, physical security, and personnel security including training and awareness. It also examines the effectiveness of contract management in cases where some ICT services are outsourced to external service providers.

3.3 Across the six agencies, the ANAO's issues papers made 112 suggestions for improvements to agencies documentation and implementation of their ICT standard operating procedures.

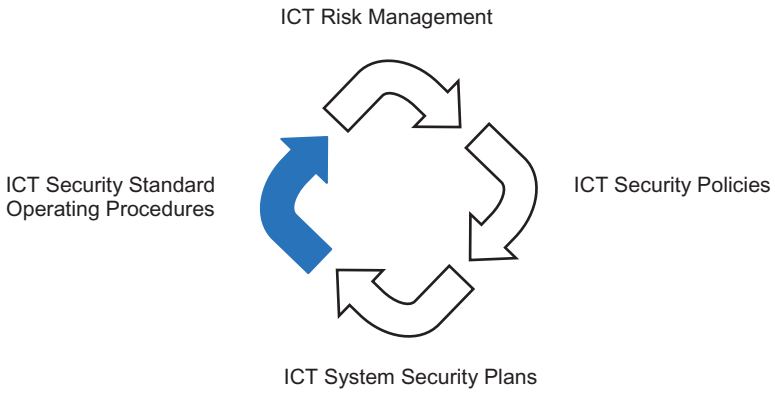
ICT security practices

3.4 Figure 3.1, as first shown in Chapter 1, illustrates the third set of ACSI 33 ICT documentation requirements. The blue arrow represents the document requirements examined in this chapter.

[41] ACSI 33, 2.6.5.

Figure 3.1

ACSI 33's Information and Communications Technology security documentation requirements



Source: ANAO analysis taking into account the requirements of ACSI 33.

Access control

3.5 Access controls are the procedures by which agencies grant and limit access to information and systems. This is an important control to secure and protect information accessible through the Internet.

3.6 ACSI 33 states agencies must ensure that all users of classified systems be uniquely identifiable and authenticated on each occasion they access those systems.[42] ACSI 33 also states that passwords for authentication should be a minimum of seven characters, and privilege accounts should be controlled, accountable and kept to a minimum.[43] Access controls need to be documented, implemented, and reviewed at regular intervals.

3.7 Of the six agencies audited, the ANAO found that each agency had documented their access controls. However, agencies' access controls did not always comply with ACSI 33, for example:

- one agency used generic passwords for new staff;
- one agency had mixed password rule settings for its different systems; and

[42] ACSI 33, 3.6.6.

[43] ACSI 33, Chapter 6, Part 3.

- three agencies did not appropriately administer user account privileges.

3.8 Providing generic passwords for new accounts increases the potential for other staff to access these new accounts without the knowledge of the account owner. Also, passwords that do not comply with the minimum requirements of ACSI 33, weaken the agency's security, making it easier for passwords to be determined and information and/or systems to be accessed.

3.9 Inappropriate access controls increase the risk of fraud and disclosure of information to unauthorised individuals. Agencies with inappropriate access controls risk compromising their information, data, and systems; and jeopardise the confidentiality, integrity and availability of their information and services.

Auditing system event logs

3.10 Auditing of system event logs[44] involves reviewing and analysing data to detect breaches in security and attempted network intrusions. Breaches can originate from within or outside an agency. Agencies that audit their system event logs are informed of the adequacy of security controls, and are well placed to take any further action required.

3.11 ACSI 33 requires agencies' system event logs to be audited and protected. Agencies should also have a sufficient number of adequately trained personnel and tools to analyse all system event logs for security breaches and/or attempted intrusions.

3.12 Of the six agencies audited, the ANAO found that:

- two agencies did not have a process for regular review of their system logs;
- two agencies audited their logs only when incidents occurred; and
- one agency did not review audit reports produced by a service provider.

3.13 Agencies that do not review their system logs in compliance with ACSI 33 increase the risk of not noticing security events, weakening the ability of management to make informed and timely decisions.

---

[44] A log is a file that lists certain events that have occurred. For example, a log might list each time a person tries to log on to a computer network and fails.

3.14 The ANAO also concluded that one of the three agencies from the 2001 audit had implemented the recommendation from the audit on regularly reviewing event logs.

3.15 The ANAO reinforces the importance of agencies following DSD's advice to regularly review and analyse their system event logs. This suggestion supports Recommendation 5 of the ANAO's *IT Security Management* audit report.[45]

Change management

3.16 Changes to ICT need to be controlled, particularly where a change has the ability to affect security.[46] The ANAO found that all audited agencies had documented change management procedures, with one agency's change management procedure representing sound practice. This agency had a documented change management process that coordinates requests, requires approval and authorisation, and tracks changes to computer systems.

Incident detection and response

3.17 An ICT security incident is an event that impacts on the confidentiality, integrity and/or availability of information or a system through an act of unauthorised access, disclosure, modification, misuse, damage, loss or destruction. Incidents can come from within or outside an agency.

3.18 ACSI 33 states the requirements for incident detection and response.[47] The ANAO found that five of the six agencies audited had documented procedures. However:

- one agency did not have a documented procedure;
- one agency had procedures scattered across several documents; and
- one agency's procedure was in draft form.

3.19 The ANAO considers that not documenting incident detection and response procedures increases the risk of a security breach not being appropriately managed. For example, if malicious code is detected, staff may not know how to respond, and the problem could spread further within the

---

45 Op. cit., ANAO Audit Report No. 23 2005–2006, Recommendation 5, p. 17.

46 ACSI 33, 2.8.6 to 2.8.10.

47 ACSI 33, Chapter 8, Part 3.

agency's network, taking longer to remedy. This could lead to interruptions to services they deliver to the community through the Internet.

Hardware security

3.20 Hardware security covers the handling, maintenance and disposal of the physical components of computer equipment such as laptops and other ICT equipment, for example, hand held devices, in a manner that does not disclose agency information.

3.21 ACSI 33 states the minimum requirements for handling, maintaining, and disposing of computer equipment.[48] The ANAO found weaknesses in the ways in which the six agencies audited managed their hardware security, for example:

- one agency had no documented procedures for the management of hardware security;
- three agencies did not have security classification labels on their hardware. Security labels provide a level of protection for the storage and handling of hardware, and limit the potential for the disclosure of information (accidentally or intentionally) to unauthorised individuals;[49]
- one agency had no documented approval process for maintenance and repair of hardware; and
- hardware security was not appropriately covered in one ICT contract.

3.22 Inadequate management of hardware increases the risk of misuse, accidental disclosure or theft of an agency's information, or fraud.

New technology

3.23 ICT is rapidly changing with existing devices being upgraded and new devices being introduced by agencies and their personnel. These changes are assisting agency productivity and service delivery through providing staff with the ability to transfer information more quickly, store greater volumes of information and making data easier to access.

---

[48] ACSI 33, Chapter 4, Part 3.

[49] Hardware containing information must be classified at or above the classification of the information stored on the hardware, ACSI 33, 3.4.9.

3.24 New technology introduced by agencies and/or their personnel include, for example:

- storage hardware – new portable storage devices, including Universal Serial Bus (USB) keys, DVD burners and portable media players;
- Internet telephony – telephone calls using the Internet as the transmission medium;
- wireless connections – network connections where there is no physical wired connections;
- biometrics – authentication techniques that rely on biometric identification, for example, fingerprints, face, iris;
- radio frequency identification – technology that incorporates small electronic tags for tracking and identification; and
- personal electronic devices – voice and data services, including video and email, using mobile telephones.

3.25 In addition, agencies and their personnel are installing new software: for example, installing software on a desktop computer that enables a hand held device to transfer information to and from a desktop computer.

3.26 Most of these new devices can be used to connect to the Internet, increasing the risks of agency information and/or systems being misused. For example, agency personnel using USB keys can remove or add information to an agency's network. This provides the opportunity for malicious code to be introduced to an agency's network.

3.27 Within the six agencies audited, the ANAO found that there were shortcomings in the management of the introduction and use of new technology hardware and software. For example:

- policy development and supporting procedures for the introduction of new technology, such as USB keys, was generally poor. Where it existed, compliance within agencies was also often poor;
- personnel in one agency were found to be using USB keys to move data from one system to another without documented controls; and
- one agency had developed procedures for procuring USB keys. However these were not derived from a risk assessment and, accordingly, were incomplete.

3.28 The ANAO also found limited evidence that the agencies it audited were balancing potential benefits against risks. Ordinarily, these would be documented in a business case.

3.29 Agencies in managing new technology should conduct risk assessments and develop and implement policies, plans and procedures for their use, and better manage risks to their business.

Recommendation No.2

3.30 The ANAO recommends that agencies develop business cases for introducing new technology, and include how they balance potential benefits against potential risks.

Australian Customs Service response

3.31 Agreed.

Australian Federal Police response

3.32 Agreed.

Australian Radiation Protection and Nuclear Safety Agency response

3.33 Agreed.

Department of Employment and Workplace Relations response

3.34 Agreed.

Department of Industry, Tourism and Resources response

3.35 Agreed. DITR agrees with the recommendation. DITR has taken the approach of assessing new technologies on their merits and will introduce requirements for documenting the current assessment of benefits versus risk. The requirements will be incorporated in the development of project and associated risk management plans.

Medicare Australia response

3.36 Agreed**.** The introduction and use of new technology will emulate the above recommendation before gaining endorsement for use in our corporate environment. Introduction of new systems and technology are subject to IT Security review and clearance before implementation.

Remote access

3.37 Remote access is any access to an agency ICT system from a location not within the physical control of that agency, such as from a staff member's

home.[50] Agencies use remote access for reasons of efficient and flexible work practices: for example, agency personnel then have the ability to access agency information when working offsite.

3.38 ACSI 33 requires that agencies that allow users remote access to systems containing classified information must ensure that: the identities of users are authenticated at the start of each session; users are given the minimum system access necessary to perform their duties; users cannot view or download information that exceeds the classification of the remote user's system; and any data transferred is appropriately protected during transmission and at the remote user's end.[51]

3.39 The ANAO examined remote access procedures in three of the six agencies, and found:

- one agency had documented its remote access procedures;
- one agency had not documented its remote access procedures; and
- one agency used a remote access solution that did not comply with ACSI 33 requirements, and its procedures were not well enforced.

3.40 Inadequate management of remote access increases the risk of the misuse or theft of an agency's information, or use of the agency's computer systems to commit fraud.

Physical security

3.41 Physical security covers storage and protection of classified information and communications equipment including desktop and server computers, from both internal and external threats.

3.42 The Joint Committee of Public Accounts and Audit inquiry report[52] stated:

> The question of the physical security of the Commonwealth's IT equipment, and the data stored on it, sprang into prominence during the course of the inquiry. Evidence taken by the Committee in another inquiry and press reports of the theft of two file servers from Customs underlined the vulnerability of IT equipment and the consequent threat to data security.

---

[50] ACSI 33, 3.10.42.

[51] ACSI 33, 3.10.43.

[52] Op. cit., Report 399.

> The Committee's concern was increased when evidence came to light of a serious security breach by Telstra Enterprise Services, when backup tapes for several departments disappeared – presumed dumped as rubbish.

3.43 ACSI 33 requires agencies to have policies, plans and procedures that address the management of physical security incidents, and to advise staff to report all physical security incidents to the information technology security adviser.[53] ACSI 33 also requires server rooms to be separate from general user areas, with access limited to authorised staff, and it requires agencies to develop site security plans and standard operating procedures for their server rooms.[54]

3.44 The ANAO found that, in the main, each of the six agencies audited had adequate physical security. However, there were minor weaknesses in all agencies that included:

- server rooms[55] not certified in compliance with ACSI 33 requirements;[56]
- hardware not adequately secured;
- visitors not escorted; and
- staff not visibly displaying security passes.

3.45 The ANAO suggests that agencies advise their personnel on physical and personnel security procedures, and ensure server rooms are secured in accordance with ACSI 33 requirements.

Personnel security including training and awareness

3.46 Agency personnel with access to computer systems require training in their responsibilities, and knowledge of potential security risks and counter measures.

3.47 The ANAO found ongoing ICT security training was not provided in four of the six agencies audited.

3.48 The ANAO suggests that agencies provide ongoing security training to staff and contractors, and include mechanisms to help staff understand security policies.

---

53 ACSI 33, 3.1.49

54 ACSI 33. 3.1.19.

55 A server room is a space containing servers and any associated communications equipment, ACSI 33, 3.1.18.

56 ACSI 33, 3.1.26 and 3.1.27.

Contract management

3.49 The ANAO examined contract management arrangements in four agencies that outsourced management of part or all of their ICT services, including Internet services. The agencies were ACS, AFP, DITR and Medicare Australia.

3.50 The PSM states that:

> When outsourcing a function, agencies remain accountable for the efficient and secure performance of that function. Each agency must ensure that appropriate security is provided for all Australian Government functions and official information. The agency must ensure that the contracted service providers are fully aware of the agency's security policy and guidelines. The agency needs to ensure that the contractor undertakes appropriate security procedures when handling official information and performing Commonwealth functions. In the case of security classified information, there are minimum standards for its handling and storage…[57]
>
> the contract must clearly state that the contractor is required to comply with the minimum standards for the protection of security classified information, detailed in the PSM.[58]

3.51 The ANAO examined two elements of contract management:

- responsibility for the development and maintenance of security documents; and
- the contractors' policies and procedures for handling classified information.

Development and maintenance of security documentation

3.52 A well written contract is fundamental in ensuring the contractor will adhere to the agency's requirements when handling security classified information. Even though an agency has outsourced its contract management, the agency is still responsible for the service and the security of the information.[59]

---

[57] Attorney-General's Department, *Commonwealth Protective Security Manual 2000*, Canberra 2000, Part A, Protective Security Policy, 2.8, A9.

[58] Attorney-General's Department, *Commonwealth Protective Security Manual 2000*, Canberra 2000, Part F Security Framework for Competitive Tendering and Contracting (CTC), 6.8, F59.

[59] PSM, Part A, clause 2.8.

3.53 The ANAO found that some contracts in two of the agencies audited:

- contained unclear statements on responsibility for development of ICT documentation and procedures;
- had no provision for handling classified information in compliance with the government's requirements; and
- contained insufficient detail for the agency to adequately monitor the service provider's performance.

3.54 The ANAO also found weaknesses in administration of the contracts in three of the agencies, which included:

- one agency did not have a copy of its contract for management of its website;
- in one agency the agency/contractor meetings were undertaken in an ad hoc manner;
- one contractor did not provide the agency with full access to the contractor's documentation on the security of the agency's information; and
- in one agency the service provider provided reports containing aggregated data and little agency specific information.

Service provider security procedures

3.55 The ANAO found that three of the four agencies for which firms provided ICT services had adequate procedures for handling classified information.

3.56 The ANAO also found that one of the service providers was not developing and maintaining ICT security standard operating procedures in accordance with the contract. The ANAO suggests that all agencies review their contract terms and conditions, and determine whether or not, the service providers are adhering to contract requirements.

Recommendation No.3

3.57 The ANAO recommends that agency Information and Communications Technology contracts include:

(a) requirements for contractors to comply with Australian Government security policies, as defined in the Attorney-General's Department's and the Defence Signals Directorate's policy documentation;

(b) agency's requirements for security reporting;

(c) a statement as to who is responsible for developing and maintaining Information and Communications Technology security plans and procedures; and

(d) reporting and performance measurement requirements.

Australian Customs Service response

3.58 Agreed.

Australian Federal Police response

3.59 Agreed.

Australian Radiation Protection and Nuclear Safety Agency response

3.60 Agreed.

Department of Employment and Workplace Relations response

(a) Agreed. DEWR has implemented these requirements. For example, DEWR's contract for the DEWR Data Centres requires the service provider to comply with all DEWR security requirements and procedures. These, of course, include compliance with the PSM and ACSI 33.

(b) Agreed. DEWR has implemented these requirements. To continue the above example, DEWR's Standard Operating Procedures for the Data Centres detail security reporting requirements.

(c) Agreed. This is documented in DEWR's IT Security Policy.

(d) Agreed. DEWR has implemented these requirements. In the situation with the Data Centres, any security issues reported are passed on to the ASA and the Department's Executive Security Committee. Where required, incidents would be reported under the DSD scheme, ISIDRAS.

Department of Industry, Tourism and Resources response

3.61 Agreed. DITR agrees with the recommendation. DITR suggests that DoFA consider the incorporation of the above requirements in the standard Government Information and Communication Technology contracting framework.

Medicare Australia response

3.62 Agreed.

a) compliance statements, as defined above, are included in all agency ICT contracts.
b) security reporting requirements are considered to be as defined by ACS133.
c) defined by agency IT Security policy.
d) included in current ICT services contract.

4. ANAO Testing of ICT Security

This chapter examines the results of assessments of desktop and server computer standard operating environments, and email filtering in ACS, AFP, ARPANSA, DEWR, DITR and Medicare Australia.

Introduction

4.1 Agencies' desktop and server computer standard operating environments face the same risks as outlined in Chapter 1, such as infection of information and systems by malicious code. Failure to manage these risks can have wide-ranging consequences for agencies and their performance, including:

- unauthorised disclosure or alteration of confidential data;
- unauthorised disclosure of clients' personal details;
- financial loss through online fraud; and
- financial loss by not having systems or data available for use.[60]

4.2 The testing of each agency's desktop and server computers, and email filtering security controls was conducted by DSD's Computer Network Vulnerability Team.

Desktop computer standard operating environment

4.3 The desktop computer standard operating environment is the way in which the agency sets up its desktop computers for use across the agency. If not appropriately protected, the desktop computer environment may contain vulnerabilities that have the potential to be exploited. For example, attacks on the desktop computer environment can come from emails received through the Internet, which have the ability to exploit weaknesses in the operating system.

4.4 For all six agencies in its sample, the ANAO assessed the following desktop computer standard operating environment controls: access controls, auditing of system event logs, and desktop computer security. [61]

4.5 The ANAO identified 90 desktop computer related risks across the six agencies. Of these, 15 per cent were high level risks, 52 per cent were medium

[60] Op. cit., Victorian Auditor-General's Office.

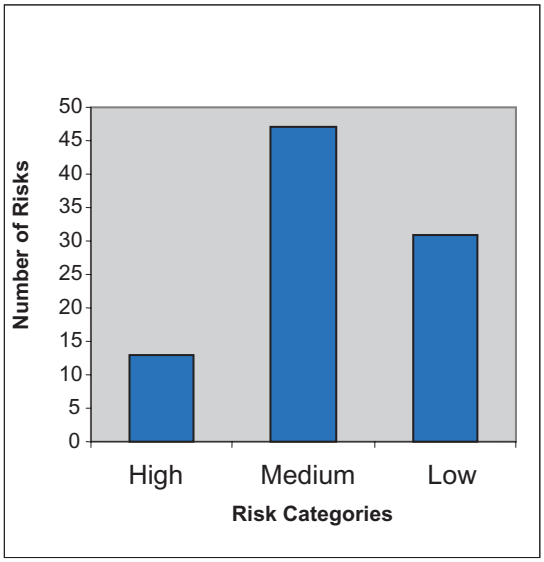
[61] Desktop computer security covers the security of the standard operating environment.

level risks and 33 per cent were low level risks. The ANAO's issues papers (provided separately to each of the six agencies) made 235 suggestions for improvement.

4.6 Figure 4.1 indicates the number of security risks identified in agencies' desktop computer standard operating environments.

Figure 4.1

Desktop computer standard operating environment risks in the six agencies audited



Source: Information provided by DSD, December 2005.

Note: High risk indicates a software vulnerability or misconfiguration that may allow the system to be compromised, for example, users with more access rights than required for their work, or there may be evidence that a compromise has taken place.

Medium risk indicates a possible software vulnerability that could allow the system to be compromised. For example, system event logs that do not hold and record enough information, and are audited in an ad hoc manner.

Low risk indicates an area that does not conform to better practice, but is not necessarily a vulnerability. For example, unnecessary software installed on the desktop computer.

4.7 The ANAO informed the respective agencies about these high-level risks during fieldwork, and the agencies advised that they would examine the problems.

Access controls

4.8 As explained in Chapter 3, access controls limit user access to information and systems. Inappropriate access controls increase the risk of unauthorised access to and misuse of agency information and/or systems. For

each of the six agencies in its sample, the ANAO assessed desktop computer access controls, such as screen savers that prohibit access after a certain time.

4.9 The ANAO found good examples of access controls in all six agencies that included:

- a limited number of users in the administrator group;[62]
- separate accounts for users with more privileges; and
- a process where, after a set number of failed attempts to log on, the user is locked out.

4.10 However, a particular area of concern was that staff in two of the agencies had more access rights than required for their work. These additional rights allowed personnel to more easily bypass security controls, increasing the risk of system compromise.

Internet access

4.11 ACSI 33 recommends that agencies block unwanted content from being downloaded from the Internet.[63] The ANAO found personnel in two of the six agencies audited were able to download from the Internet information of their choice. This could lead to the downloading of malicious code, leaving these agencies' computer systems open to infection.[64]

Auditing system event logs

4.12 As discussed in Chapter 3, producing and analysing system event logs[65] is an important part of detecting security breaches. Agencies should produce and review their logs as part of regular management of their systems.[66]

4.13 The ANAO found inadequacies in the auditing of the desktop computer system event logs, for example:

- not enough information was recorded and held for auditing, making it difficult to audit security incidents;

---

[62] An administrator group refers to a select group of ICT personnel that has privileged access to information, data and/or resources.

[63] ACSI 33, 3.5.9.

[64] Op.cit., Malicious code is software.

[65] Op. cit., A log is a file that lists certain events that have occurred.

[66] ACSI 33, 3.5.30.

- logs were not of sufficient size to collect and store all relevant information; and
- logs were audited in an ad hoc manner, making it difficult to determine what is 'normal' system activity and what constitutes potential malicious activity.

4.14 The risk of an agency not detecting security incidents increases if the agency does not manage and review logs. Then the agency may not notice important security events, and controls may not be put in place to protect against future incidents of a similar nature.

4.15 The ANAO suggests that agencies produce, review and archive logs that record exceptions and other security events to help detect and manage security incidents. This suggestion supports Recommendation 5 of the *IT Security Management* audit report.[67]

Desktop computer security

4.16 Securing the desktop computer standard operating environment involves, for example, installation of additional security barriers and security software. It can also involve the administrator regularly strengthening the security features of software used on the desktop computer when the software vendor releases new security measures.

4.17 Desktop computer security measures can minimise or even eliminate potential vulnerabilities. ACSI 33 states that agencies should monitor relevant information sources, for example, software vendor websites, about new vulnerabilities, available patches and security measures for its software and hardware. When agencies discover vulnerabilities that affect their systems, they should take corrective action and apply security patches or other measures that address those vulnerabilities.[68]

4.18 For all six agencies audited the ANAO assessed their hardware security, patching and software installed on their desktop computers.

Hardware security

4.19 To appropriately secure an agency's desktop computer standard operating environment agencies should develop and implement risk

---

[67] ANAO Audit Report No. 23 2005-06, (2005), *IT Security Management*, ANAO, Recommendation 5, p. 17, Canberra, available at <www.anao.gov.au>.

[68] ACSI 33, 3.3.23.

assessments, policies, plans and procedures for desktop computers used by staff. For example, limiting the use of USB keys reduces the potential for staff to remove information from the agency's network without authorisation.

4.20 The ANAO noted that most of the agencies audited allowed the use of USB keys to be connected to the agencies' desktop computers. Use of USB keys increases the risk of inappropriate material or software being introduced to the desktop computer and removal of sensitive material.

4.21 The ANAO suggests that agencies develop appropriate risk assessments, policies, plans and procedures for managing desktop computer hardware devices.

Patching

4.22 A patch is where additional software is installed as protection. Maintaining patches for the desktop computer reduces the risk of a security breach. The ANAO examined each agency's process for updating and implementing desktop computer patching.

4.23 The ANAO found that one agency had a well-developed patch management process that automatically applied patches to desktop computers after testing and authorisation. Not all agencies had installed patches that should have been installed, leaving their desktop computers more vulnerable. Not having an appropriate level of patching increases the risk of desktop computer vulnerabilities being exploited by hackers and by staff, inadvertently or deliberately.

4.24 The ANAO also examined whether the three agencies audited in the ANAO 2001 audit (ACS, ARPANSA and DEWR) had implemented the audit recommendation on installing security patches in a timely manner. The ANAO found that these agencies had not fully implemented this recommendation. However, the ANAO noted that there are valid reasons for not implementing patches that include: testing shows the patch to cause other problems in the desktop computer standard operating environment, or simply that they were still testing prior to application of the patch.

4.25 The ANAO suggests that agencies review their level of patching and, where required, install patches on vulnerable systems in accordance with the agency's change management process.

Installed software

4.26 Most software applications[69] have security weaknesses that require specific controls. If agencies do not implement these controls, then they are more vulnerable than otherwise. One way to reduce the risk is only to install software that supports business requirements.

4.27 For all six agencies audited, the ANAO examined software installed on the agencies' desktop computer standard operating environment, and found:

- one agency did not have controls on desktop computers to prevent users from installing and using unapproved programmes; and
- one agency had software settings which could allow malicious code to infect the desktop computer and be passed on to other desktop computers.

Server standard operating environment

4.28 The ANAO assessed the following web server standard operating environment security controls: access controls, auditing system event logs, and web server security.[70]

4.29 There were 31 risks (as defined by DSD[71]) identified in the agencies' web servers of which 3 per cent were high level risks, 32 per cent were medium level risks and 65 per cent were low level risks. The ANAO made 51 suggestions for improvements.

4.30 Figure 4.2 indicates the number of high, medium and low level risks identified in the web servers examined in the six agencies.

---

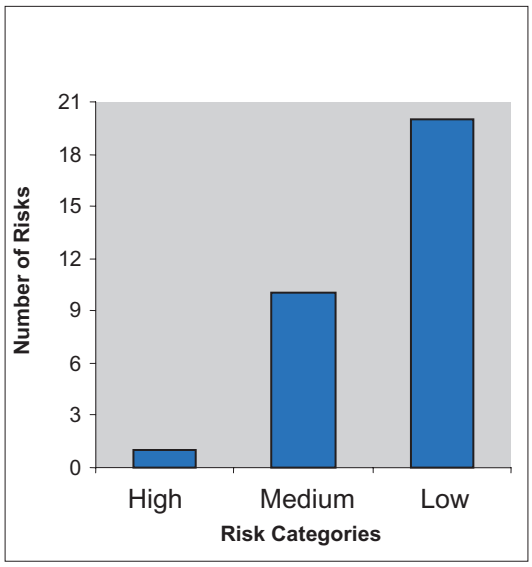
[69] Software relates to applications installed on the desktop, for example, computer programmes for word processing.

[70] Web server security covers the standard operating environment.

[71] Op. cit., High risk indicates a software vulnerability.

Figure 4.2

Server standard operating environment risks in the six agencies



Source: Information provided by DSD, December 2005.

Note: High, medium and low level risks have the same meaning as defined under Figure 4.1.
An example of a high risk is inadequate web server patching.
An example of a medium risk is inadequate log size and inadequate processes for reviewing security events.
An example of a low risk is inadequate password settings.

4.31 The majority of server risks were minor. However, the ANAO identified one serious risk in one agency. The agency was notified of the problem.

Access controls

4.32 For each of the six agencies audited, the ANAO examined web server access controls.[72] The ANAO noted that most agencies had implemented appropriate web server access controls. Controls included sound management of web server accounts, no unnecessary accounts, minimal numbers of users in the web server administrator group, appropriate password policy,[73] and logon banners[74] displayed to all users as they logged on to the web server.

---

[72] Examples of access controls include use of passwords and suspension of access after a specific number of unsuccessful logon attempts.

[73] ACSI 33, 3.6.11.

[74] Logon banners appear when a user turns on the computer; a prompt appears requiring the user to enter their password and user identifier, to access the web server.

4.33 However, one agency had shared user accounts to manage its web server. This meant that any actions performed on the server could not be directly attributed to an individual. Therefore, any auditing of the server would only identify the account that triggered the event, but not the individual user.

Auditing system event logs

4.34 The ANAO examined the auditing of web server system logs. The ANAO found that three agencies had well-developed processes for managing and reviewing web server system logs. However, the ANAO found some weaknesses that included:

- one agency had inadequate log sizes;
- two agencies did not log important security related events; and
- one agency had no defined processes for reviewing logs.

4.35 Agencies increase the risk of Internet security incidents if they do not manage and review their web server logs. Inadequate log size may lead to important information being overwritten before it is reviewed or archived. The agency would then be unable to identify the reasons for some security incidents, thereby losing information on how to combat similar problems. If agencies do not review their logs, they may be unaware of incidents occurring. For example, when a server has a security related problem, it is likely that some unusual activity would occur prior to or during the event. If this information is logged and periodically reviewed by an administrator, the likelihood of identifying the problem is greatly increased.

Web server security

4.36 Securing the web server, including patching, involves reduction and/or elimination of potential vulnerabilities within the web server. ACSI 33 states that agencies should secure and patch web servers.[75]

Patching

4.37 Hackers are continually finding new ways to penetrate agency servers through the Internet. Knowledge of particular vulnerabilities spreads quickly, and many hackers target these. Therefore, when agencies discover

[75] ACSI 33, 3.5.29.

vulnerabilities that affect their web servers, they should take corrective action and apply security patches that address them.

4.38 Most of the six agencies audited had implemented appropriate patching. However, two agencies had not installed server patches that should have been installed, leaving the server more vulnerable. For example, if an agency does not implement patches in a timely manner, it increases the risk of a successful penetration of the agency's website. This, in turn, increases the risk that web servers will be defaced and an attacker could gain control of the web server, using it for the attacker's own purposes.

4.39 The ANAO also examined whether the three agencies audited in the ANAO 2001 audit had implemented the recommendation on installing security patches in a timely manner. The ANAO found one agency had not fully implemented this recommendation in relation to web server patching. However, as stated earlier in the chapter there are valid reasons for not implementing patches in a timely manner, such as where testing shows the patch to cause other problems in the server standard operating environment.

4.40 The ANAO suggests that agencies apply web server patches, unless they are found to cause problems with the functionality of the web server, in accordance with their change management process.

Recommendation No.4

4.41 The ANAO recommends that agencies review their compliance with the *Australian Government Protective Security Manual* and the *Australian Government Information and Communications Technology Security Manual*.

Australian Customs Service response

4.42 Agreed.

Australian Federal Police response

4.43 Agreed.

Australian Radiation Protection and Nuclear Safety Agency response

4.44 Agreed.

Department of Employment and Workplace Relations response

4.45 Agreed. This is necessarily an ongoing exercise because these document are regularly updated.

Department of Industry, Tourism and Resources response

4.46 Agreed. DITR agrees with the recommendation. DITR will take steps to ensure the development of new systems and processes results in outcomes that are compliant with the PSM and ACSI 33. DITR will review on an ongoing basis existing arrangements for compliance.

Medicare Australia response

4.47 Agreed. There is an ongoing commitment to comply with the above mentioned manuals. Fulfilling compliance will be met by the application of risk management practices to assess whether new or changing environments will negatively impact the agency risk profile. In turn the ICT Security Plan and procedures are updated to reflect the ongoing quarterly changes to the ACSI 33.

4.48 The agency has in place a Security Steering Committee which ensures security matters are considered in line with the PSM and ACSI 33.

Email filtering

4.49 Email is increasingly being used to deliver malicious email attachments that, for example, take advantage of weaknesses in desktop computers. Agencies filter emails to eliminate receipt of and/or sending of unsolicited emails or emails with potentially malicious attachments. Emails have the ability to:

- infect systems and data through malicious code;[76] and
- limit access to information and data.

4.50 As part of the audit methodology, emails were crafted and sent to auditee agencies to test whether they bypassed email filters, highlighting any deficiencies in the agencies' email filtering policies or applications. The ANAO found that email filtering in all six agencies was inadequate.

4.51 Inadequate email filtering increases the risk of an attacker being able to exploit weaknesses in the desktop computer. Agencies also risk malicious emails being used to collect confidential organisational and personal information.

4.52 While email attachments are a frontline source for the transfer of malicious content, there are other avenues such as USB keys and CDs that can

[76] Op. cit, Malicious code.

be used by agency personnel to transfer malicious code on to desktop computer.

Recommendation No.5

4.53 The ANAO recommends that agencies develop and implement policies that permit them to block potentially malicious emails.

Australian Customs Service response

4.54 Agreed.

Australian Federal Police response

4.55 Agreed.

Australian Radiation Protection and Nuclear Safety Agency response

4.56 Agreed.

Department of Employment and Workplace Relations response

4.57 Agreed. DEWR has email filters in place. The policies for the filtering and the underpinning technology are continually being reviewed as new threats emerge.

Department of Industry, Tourism and Resources response

4.58 Agreed. DITR agrees with the recommendation. DITR currently has a project underway reviewing its email blocking functionality with a view to improving the blocking of malicious emails.

Medicare Australia response

4.59 Agreed. Several system enhancements have been implemented already to inhibit SPAM and malicious emails from entering the ICT environment. Further changes are also planned and the results will be reviewed on an ongoing basis to ensure that the environment maintains its effectiveness.

Ian McPhee
Auditor-General

Canberra ACT
13 June 2006

Appendices

Appendix 1: ANAO Internet related audit reports from 2001 to 2005 and better practice guide

ANAO audit reports

- *IT Security Management* - Audit Report No. 23 2005–2006;
- *Measuring the Efficiency and Effectiveness of E-Government* - Audit Report No. 26 2004–2005;
- *Management of Internet Portals at the Department of Family and Community Services* – Audit Report No. 27 2003–2004;
- *Quality Internet Services for Government Clients—Monitoring and Evaluation by Government Agencies* – Audit Report 30 2003–2004;
- *Management of e-Business in the Department of Education, Science and Training* – Audit Report No. 33 2002–2003; and
- *Internet Security within Commonwealth Government Agencies* – Audit Report No. 13 2001–2002.

ANAO better practice guide

Internet Delivery Decisions: A Government Program Manager's Guide – ANAO Better Practice Guide, April 2001.

Appendix 2: Agencies' responses

Australian Customs Service:

Recommendation 1: Agreed.

Recommendation 2: Agreed.

Recommendation 3: Agreed.

Recommendation 4: Agreed.

Recommendation 5: Agreed.

Australian Federal Police:

AFP agrees with the recommendations and believes that they will assist the agency in the ongoing development of strong, reliable and contemporary ICT security arrangements generally, and internet security arrangements in particular.

Australian Radiation Protection and Nuclear Safety Agency:

ARPANSA welcomes and agrees with the recommendations provided in this report. The Agency has already taken actions consistent with the audit recommendations in a number of areas. The recommendations will assist in the continuing development of its Internet security control program.

The Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) recognises that information and communications technology is transforming the way agencies operate. At the same time, the range of security challenges is increasing. The challenge is to reap the benefits of this technology while ensuring internet security.

ARPANSA has completed a business continuity plan including all internet services and this has undergone desktop testing. ARPANSA will continue to improve the existing plan.

ARPANSA has a formal risk management framework which includes ICT risk assessment and documentation processes. A comprehensive review of the Agency's security risks has been scheduled in 2006, to be followed by an ICT security risk assessment. These processes will include a review of compliance with the PSM and ACSI 33. ARPANSA will continue to improve the risk

assurance model through the introduction of a whole of life risk assessment and tracking process in new ICT business initiatives.

Compliance with PSM and ACSI 33 security policies is a standard requirement in ARPANSA contracts.

ARPANSA has in place an email security policy supported by extensive audit logs and monitoring procedures. Such controls endeavour to balance business objectives and efficiency with security requirements.

Department of Employment and Workplace Relations:

The Department of Employment and Workplace Relations (DEWR) has been an active user of the Internet to deliver programmes and services as well as to achieve business efficiencies through the use of the new technology. The department has over ten years experience using the Internet and has developed innovative and award winning systems which use this technology.

In using the Internet DEWR has been aware of security issues and has strenuously applied effective treatments to identified risks. This is an ongoing exercise which has been strengthened by the department's participation in this cross-portfolio audit conducted by the ANAO.

DEWR uses commercial products to provide email filtering which is effective in meeting the department's business requirements. Blocking spam has become a critical function of this filter, but it also is used to block emails which have attachments of types that are known to put the department at risk. The effectiveness of the filtering process is regularly reviewed and the department is satisfied that the protection in place is appropriate. The types of attachments that are blocked are continually evaluated based on industry advice.

Patch management is a complex area. The department uses hundreds of different software products from multiple vendors, each of whom has different approaches in providing patches. Inappropriate application of patches can disable existing business systems. DEWR evaluates each patch as it becomes available based on the exposure to the department, the likelihood of its occurring and the potential impact of applying the patch on production systems. This assessment includes advice from the wider IT industry, but also includes testing against the software configurations that are unique to the department. Patches assessed as critical are implemented as emergency changes.

DEWR believes it is best practice to review patches prior to their application. Before patches are applied to the department's desktop fleet, extensive testing and modification of existing applications is undertaken. Without this approach critical systems could become inoperable.

DEWR participated in an audit of *Internet Security within Commonwealth Government Agencies* in 2001 and was pleased to be included in this latest audit of Internet Security. Not only does it give DEWR an opportunity to test our systems, it allows the good practices that we have developed to be shared across the Commonwealth. The department agrees with the recommendations.

Recommendation 1: Agreed. Internet services are a key component of DEWR's business continuity and disaster recover plans.

Recommendation 2: Agreed.

Recommendation 3:

(a) Agreed. DEWR has implemented these requirements. For example, DEWR's contract for the DEWR Data Centres requires the service provider to comply with all DEWR security requirements and procedures. These, of course, include compliance with the PSM and ACSI 33.
(b) Agreed. DEWR has implemented these requirements. To continue the above example, DEWR's Standard Operating Procedures for the Data Centres detail security reporting requirements.
(c) Agreed. This is documented in DEWR's IT Security Policy.
(d) Agreed. DEWR has implemented these requirements. In the situation with the Data Centres, any security issues reported are passed on to the ASA and the Department's Executive Security Committee. Where required, incidents would be reported under the DSD scheme, ISIDRAS.

Recommendation 4: Agreed. This is necessarily an ongoing exercise because these document are regularly updated.

Recommendation 5: Agreed. DEWR has email filters in place. The policies for the filtering and the underpinning technology are continually being reviewed as new threats emerge.

Department of Industry, Tourism and Resources:

DITR agrees with the ANAO's report and is currently implementing these recommendations.

Recommendation 1: DITR recommends with the recommendation. DITR is taking steps in 2006-07 to both document the coverage of Internet services within business continuity and disaster recovery plans and to provide a technical solution to maintaining its Internet services.

Recommendation 2: DITR agrees with the recommendation. DITR has taken the approach of assessing new technologies on their merits and will introduce requirements for documenting the current assessment of benefits versus risk. The requirements will be incorporated in the development of project and associated risk management plans.

Recommendation 3: DITR agrees with the recommendation. DITR suggests that DoFA consider the incorporation of the above requirements in the standard Government Information and Communications Technology contracting framework.

Recommendation 4: DITR agrees with the recommendation. DITR will take steps to ensure that the development of new systems and processes results in outcomes that are compliant with the PSM and ACSI 33. DITR will review on an ongoing basis existing arrangements for compliance.

Recommendation 5: DITR agrees with the recommendation. DITR currently has a project underway reviewing its email blocking functionality with a view to improving the blocking of malicious emails.

Medicare Australia:

In general Medicare Australia agrees with the five (5) recommendations emanating from the report. Medicare Australia is committed to meeting the requirements of the audit recommendations outlined in the final report as well as those highlighted in the preceding issues paper discussed in January as part of an exit interview.
The report identified many useful activities that we will consider introducing into our work programme for the next financial year.

Recommendation 1: Agreed
Current activity
Business Continuity and Disaster Recovery are run as half yearly cycled projects within the agency. Internet services are included to ensure end to end business continuity especially for ebusiness services. These ongoing projects, report to the Executive Officer in charge of Information Technology services.

Recommendation 2: Agreed
Current activity
The introduction and use of new technology will emulate the above recommendation before gaining endorsement for use in our corporate environment. Introduction of new systems and technology are subject to IT Security review and clearance before implementation.

Recommendation 3: Agreed
Current activity
(a) compliance statements, as defined above, are included in all agency ICT contracts.
(b) security reporting requirements are considered to be as defined by ACS133.
(c) defined by agency IT Security policy.
(d) included in current ICT services contract.

Recommendation 4: Agreed
Current activity
There is an ongoing commitment to comply with the above mentioned manuals. Fulfilling compliance will be met by the application of risk management practices to assess whether new or changing environments will negatively impact the agency risk profile. In turn the ICT Security Plan and procedures are updated to reflect the ongoing quarterly changes to the ACSI 33.
The agency has in place a Security Steering Committee which ensures security matters are considered in line with the PSM and ACSI 33.

Recommendation 5: Agreed
Current activity
Several system enhancements have been implemented already to inhibit SPAM and malicious emails from entering the ICT environment. Further changes are also planned and the results will be reviewed on an ongoing basis to ensure that the environment maintains its effectiveness.

Series Titles

Audit Report No.44 Performance Audit
Selected Measures for Managing Subsidised Drug Use in the Pharmaceutical Benefits Scheme
Department of Health and Ageing

Audit Report No.43 Performance Audit
Assuring Centrelink Payments – The Role of the Random Sample Survey Programme
Department of Family, Community Services and Indigenous Affairs
Department of Employment and Workplace Relations
Department of Education, Science and Training
Centrelink

Audit Report No.42 Performance Audit
Administration of the 30 Per Cent Private Health Insurance Rebate Follow-up Audit
Australian Taxation Office
Department of Health and Ageing
Medicare Australia

Audit Report No.41 Performance Audit
Administration of Primary Care Funding Agreements
Department of Health and Ageing

Audit Report No.40 Performance Audit
Procurement of Explosive Ordnance for the Australian Defence Force (Army)
Department of Defence
Defence Materiel Organisation

Audit Report No.39 Performance Audit
Artbank, Department of Communications, Information Technology and the Arts

Audit Report No.38 Performance Audit
The Australian Research Council's Management of Research Grants

Audit Report No.37 Performance Audit
The Management of Infrastructure, Plant and Equipment

Audit Report No.36 Performance Audit
Management of the Tiger Armed Reconnaissance Helicopter Project–Air 87
Department of Defence
Defence Materiel Organisation

Audit Report No.35 Performance Audit
The Australian Taxation Office's Administration of Activity Statement High Risk Refunds
Australian Taxation Office

Audit Report No.34 Performance Audit
Advance Passenger Processing
Department of Immigration and Multicultural Affairs

Audit Report No.33 Performance Audit
Administration of Petroleum and Tobacco Excise Collections: Follow-up Audit
Australian Taxation Office

Audit Report No.32 Performance Audit
Management of the Tender Process for the Detention Services Contract
Department of Immigration and Multicultural Affairs

Audit Report No.31 Performance Audit
Roads to Recovery
Department of Transport and Regional Services

Audit Report No.30 Performance Audit
The ATO's Strategies to Address the Cash Economy
Australian Taxation Office

Audit Report No.29 Performance Audit
Integrity of Electronic Customer Records
Centrelink

Audit Report No.28 Performance Audit
Management of Net Appropriations

Audit Report No.27 Performance Audit
Reporting of Expenditure on Consultants

Audit Report No.26 Performance Audit
Forms for Individual Service Delivery
Australian Bureau of Statistics
Centrelink
Child Support Agency
Medicare Australia

Audit Report No.25 Performance Audit
ASIC's Implementation of Financial Services Licences

Audit Report No.24 Performance Audit
Acceptance, Maintenance and Support Management of the JORN System
Department of Defence
Defence Materiel Organisation

Audit Report No.23 Protective Security Audit
IT Security Management

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 of 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

Preparation of Financial Statements by Public Sector Entities	Apr 2006
Administration of Fringe Benefits Tax	Feb 2006
User–Friendly Forms Key Principles and Practices to Effectively Design and Communicate Australian Government Forms	Jan 2006
Public Sector Audit Committees	Feb 2005
Fraud Control in Australian Government Agencies	Aug 2004
Security and Control Update for SAP R/3	June 2004
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