8

Information Technology

Audit Report No. 23, 2005-06, IT Security Management

Audit Report No. 45, 2005-06, Internet Security in Australian Government Agencies

Audit Report No. 29, 2005-06, Integrity of Electronic Customer Records

8.1 This chapter examines three ANAO reports considered by the Committee together because of their common information technology theme. Each report will be outlined individually and then common issues will be discussed.

Audit Report No 23, 2005-06: IT Security Management[1]

Background

8.2 Information technology (IT) security management is an essential part of agencies' protective security environments. The management of IT security is a key responsibility of Australian Government agencies,[2]

---

1 ANAO Audit Report No. 23 2005–06 *IT Security Management*, December 2005.

2 For the purposes of their report, the ANAO used the definition of 'agency' as provided by the *Protective Security Manual* 2005, which defines agency as including 'all Australian Government departments, authorities, agencies or other bodies established in relation to

and is necessary to protect the confidentiality, integrity, and availability of information systems and the information they hold.[3] Effective IT security management requires the development and implementation of an IT security control framework[4] designed to minimise the risk of harm to acceptable levels. Given the increasing reliance on the interconnectivity of Australian Government information systems, agencies have an additional responsibility to consider how their IT security environment may affect other government agencies as well as other parties with whom they share information.

8.3 The *Australian Government Protective Security Manual* (PSM) establishes the framework of policies, practices and procedures designed for Australian Government agencies to use in protecting Australian Government functions and official resources from sources of harm[5] that would weaken, compromise or destroy them. The PSM, which was re-issued prior to the report, in October 2005, identified the standards for protective security, and specified minimum requirements for the protection of Australian Government resources.

Audit scope and objective

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

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

---

public purpose, including departments and authorities staffed under the *Public Service Act 1999.'*

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

4 An IT security control framework is the design of management processes and supporting policies and procedures, that together provide assurance that IT security management is operating effectively.

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

8.6 The eight agencies selected for review were:

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

Overall audit conclusion

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

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

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

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

- improving the content and processes for developing and maintaining IT security policy alignment with organisational risk management processes;

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

ANAO recommendations

8.11 The ANAO made five recommendations. The eight agencies examined in the audit agreed with the recommendations.

8.12 The recommendations are based on the findings of fieldwork at the audited agencies. The ANAO considers they are likely to be relevant to all agencies in the Australian Government sector.

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

Table 8.1 ANAO recommendations, Audit Report No. 23, 2005-06- IT Security Management

IT security control framework	
1.	**IT security policy** The ANAO recommends that agencies incorporate into their information security management framework, an IT security policy that establishes an agency's IT security objectives and scope, and provides reference to supporting IT security plans, procedures and standards. In addition the policy should incorporate requirements of Australian Government policies, standards and guidelines for the safeguarding of information resources.
2.	**Compliance** The ANAO recommends that agencies strengthen IT security risk processes through the use of documented IT security risk assessments, plans and policies, and conduct periodic reviews to identify gaps between agencies' IT environments, ideal risk profile and relevant government policies, standards and guidelines.
IT operational security controls	
3.	**IT equipment security** The ANAO recommends that agencies improve IT equipment security practices by ensuring that physical and environmental security controls of computing resources are clearly stated as part of their IT security policy, and that responsibilities for protecting information resources are established and documented.
4.	**Network security management** The ANAO recommends that agencies, as a part of their IT governance arrangements, monitor the effectiveness of network security practices and controls by establishing performance measures and incorporating periodic reporting against these measures.
5.	**Logical access management** The ANAO recommends that agencies, as a part of their system access arrangements, establish standards for the logging of inappropriate or unauthorised activity and introduce routine processes for monitoring and reviewing system audit logs.

The Committee's review

8.13 The Committee held a public hearing on 23 June 2006 with witnesses from the Attorney-General's Department, the Australian Government Information Management Office, Defence Signals Directorate, Centrelink and the Australian National Audit Office, to examine both Audit Report 23, 2005-06 and Audit Report 29, 2005-06.

Responsibilities and roles

8.14 The main stakeholders in Australian Government IT Security include the Attorney-General's Department, the Department of Defence—Defence Signals Directorate and the Australian Government Information Management Office (AGIMO) within the Department of Finance and Administration.

Attorney-General's Department

8.15 The Attorney-General's Department provides expert support to the Government in the maintenance and improvement of Australia's system of law and justice, national security, and emergency management.[7]

Protective Security Coordination Centre

8.16 The Protective Security Coordination Centre (PSCC),[8] a division of the Attorney-General's Department, supports the Attorney-General by providing policy advice on protective security and delivering the various programs for which it is responsible.

8.17 PSCC manages the Australian Government's protective security responsibilities and performs a coordination role in marshalling resources in preventing, or responding to, threats to our national security.

Protective Security Policy and Training

8.18 The Protective Security Coordination Centre Policy & Services Branch is responsible for developing protective security policy.[9] The PSCC provides policy advice to the Government on protective security issues and is responsible for formulating government standards and guidelines to help Australian Government agencies create and foster a secure environment.

8.19 A major role of the PSCC is to develop and promulgate this protective security policy and to provide training in protective security. These functions are carried out by the Policy Secretariat and the PSCC Training Centre.

8.20 The Policy Secretariat develops and disseminates the *Protective Security Manual* (PSM); the principal means for disseminating Australian Government protective security policies, principles, standards and procedures.

8.21 The Policy Secretariat also provides an advisory service to Agency Security Advisers (ASAs) and Information Technology Security Advisers (ITSAs) on issues relating to protective security policy and

7 http://www.ag.gov.au/

8 http://www.ag.gov.au/agd/WWW/protectivesecurityhome.nsf/Page/About_Us (accessed 1 August 2006, Last Modified: Thursday, 3 February 2005)

9 http://www.ag.gov.au/agd/www/Protectivesecurityhome.nsf/Page/RWP566A58776B765C10CA256BAE001C5CEC?OpenDocument (accessed 1 August 2006, Last Modified: Tuesday, 21 March 2006)

practices. The ASA/ITSA Forums are held on a quarterly basis to highlight issues of interest in the security field.

8.22 The Policy Secretariat provides secretariat and research services for the Protective Security Policy Committee (PSPC); a high-level interdepartmental consultative committee comprising senior executives from agencies with a strong interest in national and non-national security matters. The PSPC coordinates the development of Government protective security policy.

8.23 Basic information technology security training is provided in conjunction with the Defence Signals Directorate (DSD). The PSCC also offers security awareness training and customised protective security courses, on a fee-for-service basis. The content of all courses and seminars is based on the PSM and associated publications.

Defence Signals Directorate

8.24 DSD is Australia's national authority for signals intelligence and information security. DSD has two principal functions: one is to collect and disseminate foreign signals intelligence (known as Sigint); the other is to provide Information Security (Infosec) products and services to the Australian Government and its Defence Force.[10]

8.25 DSD's Information Security Group plays a key role in the protection of Australian official communications and information systems. For information that is processed, stored or communicated by electronic or similar means, the role of the Information Security Group is:[11]

- to provide material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; and
- to provide assistance to Commonwealth and State authorities in relation to cryptography and communications technologies.

Australian Government Information Management Office

8.26 The Australian Government Information Management Office (AGIMO) is a part of the Department of Finance and Administration. It provides strategic advice, activities and representation relating to

10 http://www.dsd.gov.au/ (accessed 1 August 2006, Last Modified 28/06/06)

11 http://www.dsd.gov.au/infosec/index.html (accessed 1 August 2006, Last Modified 28/06/06)

the application of Information and Communication Technology (ICT) to government administration, information and services.[12]

8.27 AGIMO's functions and responsibilities include:

- supporting the work of the Secretaries' Committee on ICT (SCICT), the Business Process Transformation Committee (BPTC) and the Chief Information Officer Committee (CIOC);
- identifying and promoting the development of ICT infrastructure necessary to implement emerging Australian whole-of-government strategies;
- managing the roll-out of the FedLink system, which enables secure online communications between government agencies;
- developing an e-Government Authentication Framework to assist people in verifying electronic communications; and
- managing Gatekeeper, the Government's accreditation system for certifying digital signatures.

8.28 The Committee was informed that the role of AGIMO was to encourage agencies in the effective and efficient implementation of ICT and to coordinate the implementation of the government's e-government strategy:

> Our interest in security is in ensuring that the agencies involved in ICT have a good understanding of the frameworks and that we have security matters addressed properly when we are implementing e-government initiatives.[13]

Security controls

8.29 The ANAO describes effective implementation and management of IT security as requiring both an IT security control framework and the implementation of IT operational security controls:

> The control framework provides a management structure designed to ensure that agencies take the necessary action to manage IT security risks. Operational security controls support implementation of the control framework through

12 http://www.agimo.gov.au/about/ (accessed December 2006)

13 Mr Brian Stewart, AGIMO, Department of Finance and Administration, *Transcript of Evidence,* 23 June 2006, PA 46.

> addressing objectives of confidentiality, availability and integrity of information or data stored or transmitted.[14]

8.30 The Committee was advised that for Australian Government agencies:

> the framework for IT security begins with the protective security manual, which deals with a much broader range of protective security than just IT. Part C of it deals with information security and it refers to the ACSI document 33 which gives the more detailed specific requirement for IT security.[15]

Protective Security Manual

8.31 The Attorney-General's Department issues the Australian Government's Protective Security Manual (PSM) as the:

> principal means for disseminating Australian Government protective security policies, principles, standards and procedures to be followed by all Australian Government agencies for the protection of official resources.[16]

8.32 The PSM is contained in a single manual of eight separate but cross-referenced parts. The eight parts include Protective Security Policy, Guidelines on Managing Security Risk and Information Security.

8.33 The PSCC periodically reviews parts of the PSM as appropriate, following consultation with the PSPC and other agencies.

Australian Government Information and Communications Technology Security Manual

8.34 The Australian Government Information and Communications Technology Security Manual (ACSI 33) was developed by DSD to provide policies and guidance to Australian Government agencies on how to protect their ICT systems. There are two versions of the manual; the SECURITY-IN-CONFIDENCE version and the UNCLASSIFIED version which only contains policies and guidance for classifications below the "highly protected" level. The requirement

---

14 ANAO Audit Report No. 23 2005–06 *IT Security Management*, December 2005, p.22.

15 Mr Martin Studdert, Protective Security Coordination Centre, Attorney-General's Department, *Transcript of Evidence,* 23 June 2006, PA 45.

16 http://www.ag.gov.au/www/agd/agd.nsf/Page/RWPE30AA68A4D5313EACA2571EE000AAF9F (Date Created Tuesday, 19 September 2006, Last Modified: Monday, 22 January 2007)

for agencies to comply with the manual is incorporated into the manual.

8.35 Australian Government agencies are also required by the PSM to comply with ACSI 33.

> Agencies must consider the security implications of their IT systems and devise policy and plans to ensure the systems are appropriately protected. … even unclassified systems with no special safety, mission critical, or financial implications should have some degree of protection if a reliable or accurate service is to be maintained.[17]

8.36 The manual is released up to twice a year, and is available for download from the DSD website.

8.37 Although the ANAO were not specifically looking for inadequacies in the policy, and did not find any, they did observe that not all agency staff dealing with IT necessarily understood those policies.

8.38 The Committee is pleased to note that the ANAO and DSD are working together to clarify communication of the policies in order to assist agencies in this area.

Representativeness of sample

8.39 There were eight agencies selected for review by the ANAO in relation to this report. The Committee is aware that this is only a sample of the agencies of interest in terms of public sector IT security management, but is concerned that the results of ANAO audit may be representative of the situation more broadly.

8.40 AGIMO explained to the Committee that it coordinates a Chief Information Officer Committee (CIOC) which covers all departments of state and the major service delivery agencies; a total of 27 members. In addition, the chief information officer forum picks up those Australia Government departments not formally on the CIOC. These governance forums have received presentations on this particular audit report and have been used to promote the results and recommendations.[18]

---

17 http://www.dsd.gov.au/library/infosec/acsi33.html (Last Modified: 29/09/2006)

18 Mr Brian Stewart, AGIMO, Department of Finance and Administration, *Transcript of Evidence,* 23 June 2006, PA 46.

8.41 The Committee strongly supports the dissemination of the results and recommendations from this audit more widely, and considers the AGIMO Chief Information Officer Committee and Forum to be the most appropriate mechanisms for this.

8.42 Accordingly, the Committee makes the following recommendation:

Recommendation 15

8.43 **The Committee recommends that the AGIMO Chief Information Officer Committee and Forum formally disseminate the ANAO's recommendations from Audit Report 23, 2005-06 to appropriate agencies, including seeking updates on progress and implementation.**

Audit Report No 45, 2005-06: Internet Security in Australian Government Agencies[19]

Background

8.44 It is Australian Government policy that agencies use the internet to deliver all appropriate programmes and services.[20] This policy aims to improve government services for citizens, and to raise the efficiency and reduce the costs of these services.[21] This policy has led to government agencies significantly increasing the range, volume and complexity of services delivered via the internet.

8.45 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.

---

19 ANAO Audit Report No. 45 2005–06 *Internet Security in Australian Government Agencies,* June 2006

20 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>.

21 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>.

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

8.47 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:

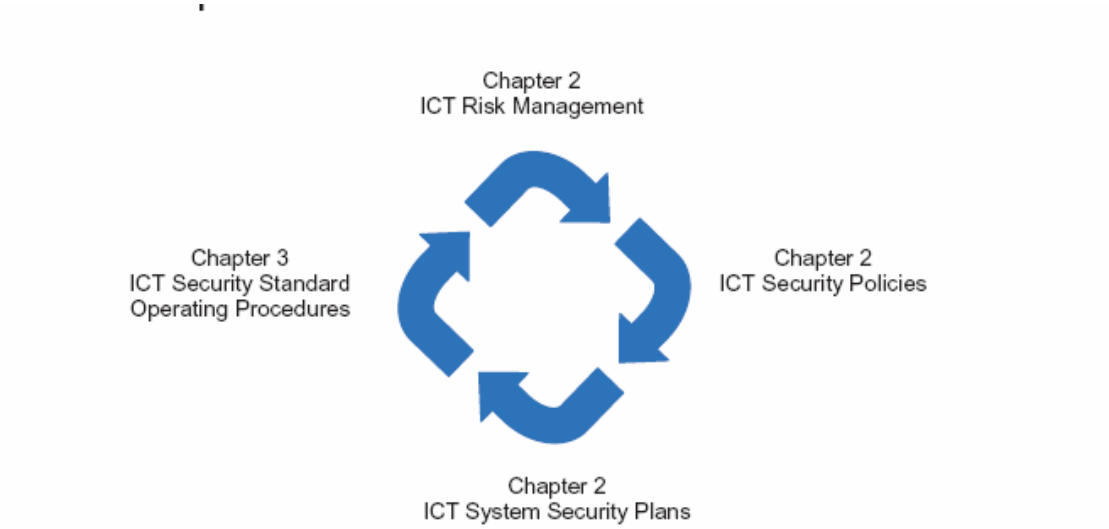
> All information systems, whether they are paper based or information and communications technology (ICT) systems, used for the processing, storage or transmission of Australian Government official information require some protection to ensure the system's integrity and reliability. This is because, even when the information processed, stored or transmitted by the system is 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.[22]

8.48 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.

8.49 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.

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

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.*

2001 performance audit

8.50 In 2001, the ANAO completed an audit of *Internet Security within Commonwealth Government Agencies*.[23]

8.51 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.

8.52 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

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

Government.[24] 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

8.53 In 2005, the ANAO completed an audit of *IT Security Management*. The JCPAA has also examined that report and the result is included earlier in this chapter. That 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.[25]

8.54 The five recommendations made by the ANAO in that report for agencies to improve ICT security are relevant to this report.

Audit objective and scope

8.55 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.

8.56 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).

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

---

24 Report 399, ***Inquiry into the Management and Integrity of Electronic Information in the Commonwealth***, JCPAA, March 2004, Parliament of Australia, Canberra, available at <http://www.aph.gov.au/house/committee/jpaa/electronic_info/report.htm>.

25 ANAO Audit Report No. 23 2005–06 *IT Security Management*, December 2005.

- 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.

8.58 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.

8.59 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.

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

8.61 An issues paper was presented to each participating agency assessing that 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.

8.62 To safeguard the security of the information held by audited agencies, the ANAO 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 trends observed across agencies.

Overall audit conclusion

8.63 The ANAO found that since the 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.

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

8.65 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.

8.66 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.

8.67 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.

8.68 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.

8.69 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.

8.70 The ANAO 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.

ANAO recommendations

8.71 The ANAO made five recommendations. The six agencies examined in the audit agreed with the recommendations.

8.72 Although the recommendations are based on the findings of fieldwork at the audited agencies, the ANAO considers they are likely to be relevant to all entities in the Australian Government.

Table 8.2 ANAO recommendations, Audit Report No. 45, 2005-06- Internet Security in Australian Government Agencies

1.	The ANAO recommends that agencies include coverage of their Internet services in their business continuity and disaster recovery plans.
2.	The ANAO recommends that agencies develop business cases for introducing new technology, and include how they balance potential benefits against potential risks.
3.	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.
4.	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.*
5.	The ANAO recommends that agencies develop and implement policies that permit them to block potentially malicious emails.

The Committee's review

8.73 The Committee received a private briefing on 6 September 2006 with witnesses from the Department of Defence, Defence Signals Directorate and the Australian National Audit Office.

8.74 As previously stated, in 2001, the ANAO completed an audit of *Internet Security within Commonwealth Government Agencies*[26] which 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 level of internet security was found to be insufficient, given the threat environment and vulnerabilities identified within a number of agency sites.

26 ANAO Audit Report No.13 2001–2002, (2001), *Internet Security within Commonwealth Government Agencies*, ANAO, Canberra.

8.75 The ANAO's objective with Audit Report 45, 2005-06 was to form an opinion on the adequacy of the management of internet security by a select group of Australian government agencies; including following up on the earlier report and subsequent JCPAA inquiry into the management and integrity of electronic information within the Australian Government.[27] The previous report looked at 10 agencies compared to the six agencies reviewed more recently. Three of the agencies were common to both audits. This enabled the ANAO to assess how well those agencies had addressed the recommendations of the earlier performance audit.

8.76 The audit assessed government agencies' activity against Commonwealth government policy. Commonwealth government policy is expressed in two key documents, the Australian *Protective Security Manual*, put out by the Attorney-General's Department, and 'ACSI 33'; the *Australian Government Information and Communications Technology Security Manual*. These documents are described in more detail later in this chapter. The audit looked at management documentation of approaches to internet security; public websites and some non-public internet connections in two places.

8.77 DSD has two roles: as the national foreign signals intelligence collection agency and the national information security agency. These two roles are complementary in that the intelligence collection side informs the information security side.

8.78 DSD does not normally look at non nationally classified systems, but can do if invited to provide advice and assistance. DSD participation in this audit enabled them to track the status of security over time to get a feel for the situation within the agencies reviewed.

8.79 The ANAO found non-compliance with government policy and guidelines in a number of areas, including weaknesses in contract management. The ANAO also found that the management of agencies' desktop computer standard operating environments could be improved and that in all cases the email filtering in agencies was considered to be inadequate.

8.80 The two major implications arising from these findings were the risk of unauthorised access to personal information, leading to privacy concerns and loss of public confidence; and the possibility of

27 Report 399, ***Inquiry into the Management and Integrity of Electronic Information in the Commonwealth***, JCPAA, March 2004, Parliament of Australia, Canberra, available at <http://www.aph.gov.au/house/committee/jpaa/electronic_info/report.htm>.

embarrassment and reduced public confidence in the agencies from any of these risks emerging.

8.81 The ANAO noted that some agencies in the sample believed that they were in compliance with government policy, when in effect they were not. The ANAO suggested that agencies need to give more attention to determining their compliance with government policy.

8.82 The Committee is disappointed to note the audit office findings that:

> For the six agencies audited, … 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[28]

8.83 The Committee is concerned that this result may be indicative of similar circumstances in other Commonwealth agencies. With that in mind the JCPAA wishes to emphasise and more formally extend the ANAO's recommendation to cover all Commonwealth agencies.

8.84 The Committee therefore recommends:

Recommendation 16

8.85 **The Committee recommends that all Commonwealth agencies, as a matter of urgency, review their compliance with the *Australian Government Protective Security Manual* and the *Australian Government Information and Communications Technology Security Manual*.**

8.86 The move to deliver services over the internet has exposed government agencies to a much greater level of risk. This is due to the fact that when connected to the internet, an avenue has been provided for access to the systems, and this is not always for legitimate reasons.

8.87 A problem described by DSD is that it is often difficult for CEOs to understand fully the importance of IT security. Non-professionals run government agencies and departments, and IT professionals must be

28 ANAO Audit Report No. 45 2005–06 *Internet Security in Australian Government Agencies,* June 2006, p. 15.

able to articulate their business requirements, and the risks, to busy CEOs under pressure and with resource constraints.

8.88 Although this audit looked at one particular aspect of security, the Committee recognises that managing the security environment is a multifaceted task. When examining internet security, a department needs to consider its people, internal practices, policies, contract management and the internet connection. This is not a simple task.

8.89 The Committee therefore makes the following recommendation:

Recommendation 17

8.90 **The Committee recommends that AGIMO provide greater assistance to Chief Executives of departments and agencies to ensure that they have the required knowledge to be fully compliant with PSM and ACSI 33 requirements.**

Trends over time

8.91 The Committee is interested in how Australian Government agencies have altered over time in terms of their approach to internet security.

8.92 The Committee was informed that agencies are increasingly using the internet to achieve two main governmental objectives: better quality client service at a lower cost.

8.93 DSD informed the Committee that over the preceding five years, government agencies had not been static. Rather they have been systematically improving their activity, including raising their level of activity to address security issues. However, they operate in an environment which is increasingly more hostile and the risks and threats are more obvious.

8.94 As government systems have increasingly become connected and interconnected, the risks have increased. Therefore the gap between agency activity and increasing risks has remained fairly stable, despite the efforts made.

ISIDRAS

8.95 Internet security is a subset of information technology security; which is concerned with the security of electronic systems, including computers, voice and data networks. 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.

> Risks to the security of government agency websites have become more acute over the past few years. …For Australian Government agencies to maintain Internet security, they need to continue to develop, improve, and review their ICT security management.[29]

8.96 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;[30]
- use or alteration of information and systems by unauthorised users.[31]

8.97 The Information Security Incident Detection, Reporting and Analysis Scheme (ISIDRAS) collects information on security incidents which affect the security or functionality of Australian Commonwealth Government computer and communication systems.[32] This allows for high-level analysis of Information Security incidents, with the ultimate aim of improving knowledge of both threats and vulnerabilities to Australian Government Information Systems and how to protect these systems more effectively.

8.98 The types of incidents that the Commonwealth agencies are asked to report include:

- unauthorised intrusion into an IT system (hacking);
- any compromise or corruption of information;

---

29 ANAO Audit Report No. 45 2005–06 *Internet Security in Australian Government Agencies,* June 2006, p. 27.

30 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.

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

32 http://www.dsd.gov.au/infosec/assistance_services/incident.html (accessed October 2006, Last Modified: 6 May 2004)

- intentional or accidental introduction of viruses to a network; and
- intentional or accidental disruption to service or damage to or loss of equipment.

8.99 The scheme uses the concept of Security Incident Categories, graded from 1 to 4, to indicate the increasing scale of severity and effect on the security and operations of a Commonwealth agency. The Protective Security Manual requires that agencies must report category 3 and 4 incidents, while reporting of category 2 incidents is optional.

8.100 Table 1.1 in the ANAO's report summarises four years' reporting of internet security incidents by Government agencies. That table is reproduced below as Table 8.3.

Table 8.3 Australian Government agencies' reporting of Internet security incidents to DSD, 2001–02 to 2004–05[33]

Security incidents	2001–02	2002–03	2003–04	2004–05	Total
Category 1 incidents (minor)					
Email scams[34]	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.

8.101 DSD advised the ANAO that the data in Table 1.1 under-represents government internet security incidents due to agencies under-reporting.[35]

33 ANAO Audit Report No. 45 2005–06 *Internet Security in Australian Government Agencies,* June 2006, p 29.

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

35 ANAO Audit Report No. 45 2005–06 *Internet Security in Australian Government Agencies,* June 2006, p. 29.

8.102 The Committee is concerned about the under-reporting by agencies and believes that more reliable data should be available to DSD so that they can appropriately monitor the risks.

8.103 The Committee therefore makes the following recommendation:

Recommendation 18

8.104 **The Committee recommends that DSD formally remind all agencies of their responsibility to comply with ISIDRAS reporting as required by the Protective Security Manual.**

Contracts

8.105 The Committee noted that ANAO recommendation number 3, relating to agency ICT contracts, included information which generally should be considered as standard requirements.

8.106 The ANAO said that this was necessary due to some of the contracts that they examined showing problems in those areas.

8.107 DSD indicated that they were already working with AGIMO to ensure that this information was being included in standard contracts. In addition, the question of who has responsibility when the service is outsourced was being examined in order to lessen the confusion in this area.

8.108 Ultimately it is the responsibility of the CEO who receives the information on internet security. The ANAO are working with DSD to raise the priority of this issue.

Audit Report No 29, 2005-06: Integrity of Electronic Customer Records[36]

Background

8.109 Like most Australian Government agencies involved in service delivery in the 21st century, Centrelink relies on large and complex information technology systems to support its extensive business

36 ANAO Audit Report No. 29 2005–06 *Integrity of Electronic Customer Records*, February 2006.

operations. The heart of Centrelink's IT systems is ISIS—the Income Security Integrated System— Centrelink's main customer database.

8.110 In 2004–05, Centrelink's IT systems performed more than 5.2 billion electronic computations and processed some $63 billion of social security payments to over six million customers. Centrelink grants approximately 2.8 million new claims each year. At September 2005, the ISIS database held information on over 23 million customers—recording details of customers' identity, circumstances and eligibility for benefits under various social security programmes. Approximately 6.2 million of the 23 million records relate to customers with a current benefit determination.[37]

8.111 In order to distinguish between customer records, a unique identifier is assigned to each record—the Centrelink Reference Number, or CRN. The information in ISIS is organised around the CRN, which links customer information in various parts of the database. For example, the CRN links information on a customer's circumstances and benefit determinations with that in the payments file.

8.112 Customer information is spread across eleven networked computing environments, with each environment, essentially, servicing a region, state or territory within Australia.[38] Centrelink's data holdings are growing at a rate of approximately 30 percent each year, and at September 2005, the ISIS database held information in over 440 billion fields, with an average of 21 000 fields of information per customer.

Audit approach

8.113 The ANAO audit examined aspects of the integrity and management of customer data stored on ISIS. In particular, the audit considered measures of data accuracy, completeness and reliability. The scope of the audit also extended to aspects of Centrelink's IT control environment—in particular, controls over data entry.

8.114 The ANAO considered Centrelink's processes and procedures for entering customer data into ISIS, including the controls surrounding customer registration and the validation of customer data. ANAO also examined Centrelink's existing data integrity error detection and reporting system.

---

37 Other records include historical records for customers previously in payment, along with records for organisations and children.

38 One of the computing environments stores information on Centrelink customers residing outside Australia.

8.115 Centrelink provided data extracts from all 23 million ISIS records. The ANAO tested the contents of a number of mandatory fields to ensure these conformed to Centrelink's business rules and specifications. The ANAO's analysis also included a check of logical relationships between various fields.[39] Centrelink customers are required to prove their identity when claiming a pension, benefit, or allowance from Centrelink. The ANAO examined details of Proof of Identity (POI) documents recorded on ISIS.

8.116 A substantial part of the ANAO's analysis involved testing the integrity of the primary key[40] of the database—the CRN. ANAO checked for the existence of duplicate CRNs—whether any given value for a CRN was associated with more than one customer—and for multiple CRNs—where an individual customer had been assigned more than one CRN.[41]

8.117 Fieldwork for the audit was primarily undertaken during April 2005 to October 2005. The ANAO acquired over 8 million lines of data, extracted from the agency's data integrity error detection system on 12 July 2005. On 13 September 2005, Centrelink provided ANAO with over 23 million lines of data extracted from the main ISIS database, in accordance with the ANAO's specifications.

Overall audit conclusion

8.118 Centrelink's customer database, ISIS, constitutes one of the largest and most complex Australian Government databases holding information about Australian citizens and residents. With over 23 million records in total, some 6.2 million records support a current benefit determination, and in most cases, payment to a customer by Centrelink.

8.119 This audit found that Centrelink could significantly improve the accuracy and integrity of data stored on ISIS. In particular, Centrelink could improve the integrity of the primary key used in ISIS, and reduce the risks associated with fragmenting customer information across multiple records. Centrelink should also remove training records and obsolete customer records from the production

39 For example, that a customer's recorded date of death did not precede his or her recorded date of birth, or that a customer's marital status (single or partnered) aligned with the payment rate for a benefit that was paid at either a single or partnered rate.

40 The primary key is a means of uniquely identifying each record within the database and a mechanism to link data across various elements of the database.

41 And, therefore, had multiple records in the database.

environment of its database. The ANAO also found that Centrelink should improve the effectiveness of its existing data integrity checking system.

8.120 The audit found that up to 30 percent of customer 'proof of identity' (POI) information recorded on ISIS was insufficient or unreliable in terms of uniquely identifying or substantiating the identity of customers. While much of this information related to historical records, the ANAO also found that this information is still relied upon to process new claims associated with those historical records. The ANAO noted that Centrelink has tightened some of the controls around POI data entry and that the quality of recently entered POI information appears to be considerably improved.

8.121 While this audit has highlighted a number of business risks arising from these data integrity issues, including the risk of duplicate or inappropriate payments to customers, the ANAO also found that Centrelink had in place a number of other controls designed to prevent inappropriate payments. Accordingly, the audit found that, while these risks exist, duplicate payments had only occurred in a small number of cases.

8.122 Therefore, given the scale and complexity of Centrelink's IT operations, and considering the information examined in the scope of this audit, the ANAO concluded that Centrelink's electronic customer records are, generally, sufficiently accurate and complete to support the effective administration of the range of social security programmes for which Centrelink is responsible.

8.123 The ANAO also recognised that Centrelink responded promptly to the matters raised during the course of this audit, and commenced a number of initiatives to address specific data integrity issues identified by the ANAO, and to generally improve the quality of data in ISIS. Key among these initiatives were projects to analyse and correct the identification of false positive results in the agency's existing data integrity error checking system, the establishment of a Data Quality Team to develop a long term strategy to improve and maintain data quality and work to comprehensively describe the effects of data integrity errors. Centrelink also undertook to review the operation of the priority rating system for data integrity errors.

8.124 In addition, Centrelink acted quickly to review cases of potential duplicate payment of customers, and to commit to resolving cases of duplicate and multiple CRNs.

ANAO recommendations

8.125 The ANAO made five recommendations, which were all agreed by Centrelink.

Table 8.4 ANAO recommendations, Audit Report No. 29, 2005-06 - Integrity of Electronic Customer Records

1.	The ANAO recommends that Centrelink improve the usefulness and effectiveness of its data integrity (DI) reporting system by: (e) ensuring the timely inclusion of new or revised DI checks whenever new software applications are released, so that the system is always checking data against current business rules; and (f) enabling the system to clearly identify DI errors associated with current customers. *Centrelink's response: Agreed*
2.	ANAO recommends that Centrelink, in order to provide programme managers with the capacity to determine the relevant priority of DI issues, including those requiring urgent or immediate attention, revise its priority rating system for DI errors, with a view to: (a) comprehensively and accurately describing the likely effects of DI errors; (b) resolving inconsistencies between the stated effects of some errors and the criteria for ascribing particular priority ratings; and (c) clearly identifying DI errors that pose the greatest risk to the efficient and effective administration of programmes and payments. *Centrelink's response: Agreed*
3.	ANAO recommends that, in order to address the range of data quality issues identified by this audit, Centrelink conducts a thorough data cleansing exercise within the ISIS database, with a view to: (a) removing training records and spurious customer records from the production environment; (b) removing or otherwise inactivating records for deceased customers from the production environment, where there is no continuing business need to retain the records (c) improving the accuracy of customers' personal information, particularly in recording the various elements of customers' name and address (d) enforcing existing business rules surrounding the use of defined legal values with certain ISIS fields (e) resolving possible anomalies in the recorded dates of birth and death for Centrelink customers identified during this audit; and (f) resolving possible anomalies in the recorded Tax File Numbers for Centrelink customers identified during this audit. *Centrelink's response: Agreed*
4.	ANAO recommends that Centrelink: (a) continues to monitor the operation of its Proof of Identity policy and the quality of POI information recorded in ISIS; and (b) progressively replaces spurious or inaccurate POI information currently recorded in ISIS with accurate information, when processing new claims or undertaking major of reviews of eligibility for existing customers. *Centrelink's response: Agreed*

5. ANAO recommends that, in order to improve the integrity of the CRN, the primary key for ISIS, Centrelink takes action to resolve:

(a) all duplicate CRNs — instances where **different** customers have been allocated the same CRN and instances where the **same** customer has a current benefit determination on two or more Centrelink computing environments;

(b) all multiple CRNs — instances where the same customer has been registered under two or more different CRNs; and; and

(c) all instances of records where a date of death has been recorded against one of a customer's duplicate or multiple records, but not the other(s).

Centrelink's response: Agreed

The Committee's review

8.126 The Committee held a public hearing on 23 June 2006 with witnesses from the AG's Department, AGIMO, DSD, Centrelink and the ANAO, to examine both Audit Report 23 and Audit Report 29, 2005-06.

Data integrity errors

8.127 As Centrelink described, the audit focussed on data integrity errors within Centrelink's customer database:

> A data integrity error is quite different from, say, an error in a payment to a customer. Data integrity errors are very specific sorts of errors and the audit was on the data integrity side of things.[42]

8.128 Centrelink notes that the audit has given data integrity a higher profile in Centrelink, which was a good outcome.

8.129 As a result of the audit, Centrelink has in place a full-time data quality team to undertake data quality runs to identify these sorts of errors. Centrelink described the main errors identified by the audit as duplicate records, multiple records, archiving, proof of identity and the tax file number issue. This involved 182,000 records which were returned requiring remediation.

8.130 At the time of the hearing, the data quality team had checked through the returned records and from the 8.2 million data integrity errors mentioned in the report Centrelink had reduced this figure to about 3.1 million. The target was to check the remaining records by February 2007, potentially requiring going back to the base documents or even contacting the customers.[43]

42 Mr John Wadeson, Centrelink, *Transcript of Evidence,* 23 June 2006, PA 40.

43 Mr John Wadeson, Centrelink, *Transcript of Evidence,* 23 June 2006, PA 43.

8.131 The Committee was concerned at the large number of errors identified in the audit. However it was pleased to note the progress being made to rectify these errors.

Inactive records

8.132 Another issue raised in the audit dealt with inactive records. Centrelink acknowledged that many of these records which existed in the major production systems were for deceased customers however used the term 'inactive' records to include those such as training records which were no longer active for other reasons.

8.133 The ANAO recommended removing or otherwise inactivating such records from the production environment, where there is no continuing business need to retain the records.

8.134 Centrelink responded to the suggestion to move the records "to environments where they would be less involved in mainstream production", by stating that this would require quite complicated IT and would be "quite a difficult thing architecturally". Centrelink stated it was investigating options relating to this issue.[44]

8.135 The Committee understands that the ANAO recommendation relating to inactive records is not a simple one to implement, however we agree with the audit office that "the existence of these records gives rise to an unnecessary risk to the integrity of Centrelink payments".[45] The Committee therefore strongly endorses the recommendation and Centrelink's prompt examination of options to address this risk.

8.136 Therefore the Committee makes the following recommendation:

Recommendation 19

8.137 **The Committee recommends Centrelink's prompt examination of options to address the risk posed by inactive records within Centrelink's major production systems.**

44 Mr John Wadeson, Centrelink, *Transcript of Evidence,* 23 June 2006, PA 43.

45 ANAO Audit Report No. 29 2005–06 *Integrity of Electronic Customer Records*, February 2006, p.19

8.138 Centrelink informed the Committee that there is an audit monitoring system in place to physically follow-up each audit office recommendation to ensure they are "embedded and in place".[46]

8.139 The Committee commends Centrelink for the close involvement with ANAO throughout the audit process, for addressing some recommendations as they were flagged by the audit office, and for their general approach to the recommendations.

Common issues

Whole of government perspective

8.140 The Committee raised the question of whether a single agency with the whole-of-government responsibility for IT issues, including internet security, might improve coordination in this area. DSD stated that the involvement of multiple agencies in setting the standards is not conducive to standardised policy and process. Additionally, using DSD to police levels of compliance was not considered to be an appropriate use of resources.

8.141 Instead, DSD supported the current model, whereby the protective security manual and ACSI 33 provide policy and advice, which it is then up to agency and department heads to follow. Once the policy and the standards have been set, and an audit function is in place, DSD can then assist departments to understand where problems exist and how to meet their obligations.

Unauthorised staff access of information

8.142 The ANAO reported that:

> A major risk to Internet security also comes from within agencies, where personnel have the potential to accidentally or deliberately change information.[47]

8.143 The Committee raised concerns regarding the unauthorised access issues within Centrelink[48] and the ATO[49] which had recently been discussed in the media. These were cases of staff that were authorised

46 Mr Bob McDonald, Centrelink, *Transcript of Evidence,* 23 June 2006, PA 43.

47 ANAO Audit Report No. 45 2005–06 *Internet Security in Australian Government Agencies,* June 2006, p. 15.

48 Welfare workers axed for spying, The *Australian*, Wednesday 23rd August 2006.

49 Tax office sacks 'spies', The *Australian*, Tuesday 29th August 2006.

to use the system, but were inappropriately accessing records (as distinct from unauthorised access of records).

8.144 DSD advised that the only available data on this is that which has been reported under ISIDRAS, as can be seen in table 8.3. After detection of such cases, it is up to the agency to decide what action is to be taken.

8.145 DSD advised that routine and effective internal audits will catch people engaging in unauthorised access activities. Rather than being focussed on catching people out, security was described as making it harder for people to access networks inappropriately and about maintaining appropriate configurations.

The access card

8.146 At the time of the Committee's review the Australian Government was proposing to introduce a single card for people to use government health and social services.[50] The card was planned to replace up to 17 existing cards, including Medicare cards, Centrelink benefit and concession cards and Veterans' cards.

8.147 While since overtaken by events, the agencies responded to questions relating to the proposed introduction of the access card. DSD representatives stated that they would be involved throughout the Access Card development process, working very closely with AGIMO and other departments in relation to the security of that database. DSD stated that there was a broad understanding of what the access card means.

8.148 AGIMO described its role in relation to the access card as;

> "about setting a whole-of-government framework for smartcards"… An important part of that framework is security and privacy, and we have been getting quite significant input from DSD, A-G's and the Privacy Commissioner on the privacy and security elements of that framework. We are working quite closely with Human Services. They are involved in the development of that framework as well and they have indicated they will be using that framework as part of the access card implementation.

50 http://www.accesscard.gov.au/ (accessed December 2006)

> Our role is very much about awareness raising, best practice and frameworks.[51]

8.149 AGIMO observed that "Whether or not to implement a smartcard is a question for the government".[52]

Levels of risk

8.150 The Committee was interested in the security control framework and its aim of minimising the risk of harm to acceptable levels, and what levels were considered "acceptable", particularly for agencies which may be considered critical due to the personal data held by them (eg. Centrelink, the Health Insurance Commission).

8.151 The ANAO explained how their audits looked at risk from the point of view of confidentiality but also availability and integrity.

> The availability requirements or acceptable levels of risk may vary for each organisation, because availability also considers things like recoverability from an IT failure or outage. Some agencies might have some systems which do not need to be recovered for seven days. Other agencies, some of the critical central providers, may expect [that] the systems are virtually always up and available. So the levels of risk that are acceptable will vary depending on what the services support.[53]

8.152 Centrelink explained that the minimum level of risk is determined after long and fairly detailed risk assessments have been done.

> The level of risk that becomes acceptable could best be described as the lowest we can possibly achieve with the resources we have available, the technologies we have available and considering the demands on us for the delivery of services. There is always a balance in all of this.[54]

8.153 The Committee is satisfied that for the agencies which appeared before the Committee, reasonable effort was expended in determining what constituted "appropriate" levels of risk for IT security.

---

51 Mr Brian Stewart, AGIMO, Department of Finance and Administration, *Transcript of Evidence,* 23 June 2006, PA 46.

52 Mr Brian Stewart, AGIMO, Department of Finance and Administration, *Transcript of Evidence,* 23 June 2006, PA 47.

53 Mr Greg Mazzone, ANAO, *Transcript of Evidence,* 23 June 2006, PA 41.

54 Mr John Wadeson, Centrelink, *Transcript of Evidence,* 23 June 2006, PA 40.

8.154 The Committee encourages all agencies to re-examine their determination of minimum IT security risk levels, to ensure that detailed risk assessments have been undertaken and a security framework is in place so that the levels are in fact appropriate.