ACT Auditor-General's Office

Performance Audit Report

Whole-of-Government Information and Communication Technology Security Management and Services

Report No. 2 / 2012

ACT AUDITOR-GENERAL'S OFFICE

PA 09/03

The Speaker
ACT Legislative Assembly
Civic Square, London Circuit
CANBERRA ACT 2601

Dear Mr Speaker

I am pleased to forward to you a Performance Audit Report titled 'Whole-of-Government Information and Communication Technology Security Management and Services', pursuant to Section 17(5) of the *Auditor-General Act 1996*.

Yours sincerely

Dr Maxine Cooper
Auditor-General
8 June 2012

Level 4, 11 Moore Street, Canberra City, ACT 2601 | PO Box 275, Civic Square, ACT 2608

Telephone: 02 6207 0833 | Facsimile: 02 6207 0826 | Email: actauditorgeneral@act.gov.au

CONTENTS

List of abbreviations **1**

1. Summary and conclusion **3**

Introduction 3

Background 3

Audit objective 4

Audit conclusion 5

Key findings 6

Recommendations and response to the report 9

Acknowledgements 15

2. Whole-of-government information and ICT security management and services **17**

Responsibilities 17

Justice and Community Safety Directorate 20

Treasury Directorate 29

Approval of draft policies, and general oversight of ICT security 41

Chief Minister and Cabinet Directorate 42

Appendix A: Audit criteria, approach and method **45**

Audit criteria 45

Audit approach and method 45

Appendix B: Shared Services ICT Policies and Procedures **47**

Appendix C: Territory Records Office Recordkeeping Standards, Guidelines and Records Advices **49**

LIST OF ABBREVIATIONS

CMCD	Chief Minister and Cabinet Directorate
ICT	Information and Communication Technology
JACSD	Justice and Community Safety Directorate
Shared Services ICT	Shared Services ICT (formerly InTACT)
SEMC	Security and Emergency Committee of Cabinet
SEMB	Security and Emergency Management Branch of the JACSD Directorate
SEMSOG	Security and Emergency Management Senior Officials Group
SSGC	Shared Services Governing Committee
TRO	Territory Records Office

1. SUMMARY AND CONCLUSION

INTRODUCTION

1.1 This report presents the results of a performance audit on whole-of-government information and communication technology (ICT) security management and services for ACT Government directorates and agencies.

BACKGROUND

1.2 ICT security is a component of information security that in turn is part of an organisation's protective security.

1.3 Protective security policies guide the management of information security to ensure that the right people get the right information, at the right time, in the right location. Information security management should be part of an organisation's overall management system, based on business risk.

1.4 The ACT Government's *Protective Security Policy and Guidelines* is the overarching document that sets the broad context for all information security, including, and importantly for this audit, information and communication technology (ICT). It describes 'information' as including documents and papers; the intellectual information (or knowledge) acquired by individuals; and physical items from which information regarding design, components or use could be derived.[1] Information will comprise, but is not limited to, personal data (for example, health/medical records, criminal records and other case management records) and sensitive government documents that, if accidentally or maliciously made public may cause strategic, economic or political damage

1.5 Information security is an important, complex and challenging issue particularly as information management needs to continually respond to new technologies and community expectations.

1.6 The Australian Government's *Information Security Manual of 2010* defines information security as:

> a higher level of abstraction than cyber security and relates to the protection of information regardless of its form. Information security in government is composed of 'measures relating to the confidentiality, availability and integrity of information'.[2]

[1] ACT Government, *Protective Security Manual and Guidelines*, paragraph 3.1.2, p. 36.

[2] Australian Government Department of Defence, *Australian Government Information Security Manual,* November 2010, p.1.

1.7 The ACT Government's *ICT Security Policy* states:

> In fulfilling its commitment to the community, the ACT Government collects, receives and develops information.
>
> Information assets if lost, inappropriately amended, or disclosed to unauthorised parties have the potential to cause major disruption to the mechanisms of government of the ACT, the delivery of justice and to the national security of the Commonwealth.
>
> This policy provides a whole-of-government information security regulatory framework to ensure the ACT Government meets its obligations to protect and safeguard official information assets …

1.8 Consistency in ICT security across government directorates and agencies ensures that data are protected in the required manner and it is likely to be cost effective in that each agency does not need to invest funds in developing its own policies and procedures.

1.9 Responsibility for protective, information, and ICT security resides:

- from a policy perspective with:
  - Justice and Community Safety Directorate's Security and Emergency Management Branch (SEMB) which is responsible for managing the ACT Government's protective security policy and documentation, and supporting key security and emergency management committees;
  - Treasury Directorate's Territory Records Office which administers the *Territory Records Act;*
- from a management of technology perspective with Treasury Directorate's Shared Services Division's, Shared Services ICT Security Section which is the ACT Government's information and communication technology provider; and
- from an operational perspective each directorate and agency is responsible for ensuring policies and procedures are in place so that staff comply with whole-of-government policies in managing their ICT.

1.10 Shared Services' networks support 37 500 students and 5 000 teachers, 18 000 public servants and Canberra Institute of Technology students locally and overseas.

AUDIT OBJECTIVE

1.11 The objective of this audit is to provide an independent opinion to the Legislative Assembly on whether the administrative structures and processes for whole-of-government ICT policies and procedures are well defined, managed and communicated. In doing this relevant information security and protective security issues are also considered.

1.12 This objective is a modification of an objective that was originally adopted in February 2011. Since this date, the audit has changed due to several compounding factors.

1.13 Consideration of the implementation of ICT security policies and procedures in two directorates was originally proposed however, findings from this would not have been able to be extrapolated to all directorates or agencies. Therefore, only the part of the audit that was focused at the whole-of-government level has been progressed. A future discrete audit of directorates' and agencies' application of ICT security may be worthwhile once any recommendations from this audit are implemented.

1.14 The audit did not examine individual ICT security systems. Conclusions on the adequacy of controls over unique systems cannot therefore be extended to systems that were not subject to audit.

AUDIT CONCLUSION

The protection of the ACT Government network is robust. Shared Services ICT Security Section's security regime has successfully defended against over one million attempts to access the ACT Government's network in the nine month period to 31 March 2012. However, a breach of security did occur in relation to an externally hosted website. Future similar breaches could be minimised if all directorate and agency websites were hosted on the ACT Government network or an ACT Government endorsed supplier.

While the administrative structures and processes that support whole-of-government ICT policies and procedures are overall satisfactory there are some shortcomings. ICT security governance is based on the *Protective Security Policy and Guidelines* which is the ACT Government's pre-eminent protective security document. However it is unclear if the status of this document is well understood or if adequate processes exist to ensure that directorates and agencies are complying with it. This could, in part, be addressed if whole-of-government administrative structures and processes were better defined and readily available. It is particularly important that the role of the ACT Government IT security advisor be reinforced, its functions endorsed and supported by key cross-directorate committees and all directorates and agencies. It is also important that the ACT Security in Government Committee fulfils all of its terms of reference or a review of its terms of reference be initiated to clarify its functions. Such actions would strengthen the whole-of-government arrangements that support ICT security in directorates and agencies.

The *Protective Security Policy and Guidelines* while stating that '…standards, while not mandatory, will assist in the transition to a security culture within the ACT Government', also states that directorates and agencies 'should' and even 'must' do certain things. This ambiguity is being addressed in the review underway of the *Protective Security Policy and Guideline* by defining what is or is not mandatory. To

provide additional guidance to directorates and agencies in implementing the revised document references to international standards on information and ICT security should be included.

Despite it being a requirement, only 5% of the ACT Government's 1025 information management systems have a system security plan; and even fewer, some 2.24% have a threat and risk assessment. The reasons for this were not able to be ascertained. This is an issue that needs to be addressed.

Hand held devices, known as 'portable platforms' that can access the ACT Government networks and the internet are proliferating. New or amended policies to govern the use of new technologies are required as a matter of priority.

The ACT Government does not have an electronic records management system. The need for such a system is likely to increase.

KEY FINDINGS

1.15 Key findings are:

Responsibilities

- Whole-of-government information security roles and responsibilities and communication processes are not overall well defined and documented, this hinders communication. Such information should be readily available.
- The Senior Manager of Shared Services Information and Communication Security Section is designated as the ACT Government's IT Security Advisor by the Shared Services Governing Committee, and accepted as such by the ACT Security in Government Committee. This is a particularly important role with respect to ICT security.
- The Security and Emergency Management Branch (in Justice and Community Safety Directorate) and Shared Services ICT Security Section (in Shared Services Division), have a strong informal relationship. This facilitates linkages between protective, information, and ICT security. Accordingly it would be prudent to formalise this relationship and document communication protocols.

Justice and Community Safety Directorate

- The Justice and Community Safety Directorate's *Business Risk Management Plan* records as 'high' a risk of 'ineffective oversight of the protective security arrangements across the Territory and within JACSD' because it is unlikely, but would have major (unspecified) impacts. To control this risk, Justice and Community Safety Directorate issued the *Protective Security Policy and Guidelines*. The resulting residual risk, after this risk treatment, is judged to

be low.

- The Security and Emergency Management Branch is the lead policy agency for protective security in the ACT Government. Inter alia, it is responsible for 'creating a security culture across ACT Government through protective security policy and education'. It is the custodian of the ACT's *Protective Security Policy and Guidelines*,

The *Protective Security Policy and Guidelines*

- The ACT Security in Government Committee is currently reviewing the *Protective Security Policy and Guidelines*. The Committee intends to recommend to the Security and Emergency Management Senior Officers' Group the adoption of a subset of the 33 mandatory requirements. It is proposed that the revision of the *Protective Security Policy and Guidelines* be considered by the ACT Security in Government Committee by December 2012, and at an unspecified time later, by the Security and Emergency Management Senior Officers' Group. The Security and Emergency Management Committee of Cabinet will approve the revised *Protective Security Policy and Guidelines* following the Security and Emergency Management Senior Officers' Group's review.
- Clarifying what is and is not mandatory in the *Protective Security Policy and Guidelines* is important to ensure consistency in the implementation of policies and procedures across directorates and agencies. Adoption of the Commonwealth's approach, with points for mandatory compliance, will provide clarity.
- The revised *Protective Security Policy and Guidelines* should include references to international standards on information and ICT security to provide additional guidance to directorates and agencies.
- There is no current information on compliance with the ACT Government's *Protective Security Policy and Guidelines* across all directorates. The risk of security gaps being unnoticed and uncontrolled is increased as a result.
- The ACT Security in Government Committee's terms of reference requires it to report to the Security and Emergency Management Committee of Cabinet, via the Security and Emergency Management Senior Officials Group on the status of protective security in government agencies.
- The ACT Security in Government Committee proposes that in the future information on Directorates' and agencies' compliance with the *Protective Security Policy and Guidelines*, will be reported annually to the Security and Emergency Management Senior Officials Group.

Classification of information

- The ACT Security in Government Committee and the Security and Emergency Management Senior Officials Group have adopted the new classification

system of the Commonwealth's *Protective Security Policy Framework* (Protected, Confidential, Secret and Top Secret).

- Guidance provided in the *Protective Security Policy and Guidelines* on information classification is oriented toward hard copy classification. Currently, there is no automated method to classify electronic data held on network drives.

Shared Services Division

- Most, but not all, directorates and agencies have service level agreements with Shared Services. The model under which Shared Services information and communication technology operates intends that service delivery should be shared, with mutual responsibilities.
- Some directorates and agencies rely on securing services from the market despite Shared Services ICT being the ACT Government's preferred supplier. Centralised services are likely to afford a higher level of ICT security.
- Shared Services ICT Security Section maintains the perimeter security of the ACT Government networks and their applications. This security has proved to be robust in resisting cyber attack. In the nine months to 31 March 2012, over one million cyber attacks were repelled.
- Hand held devices, known as 'portable platforms' that can access the ACT Government networks and the internet are proliferating. Use of these devices has raised a number of questions, such as who owns the data on a device provided to an employee. Shared Services ICT Security is drafting and amending policies to govern the use of these mobile devices and other emerging technologies. This is supported and should be given priority.
- There is great scope for expanding the use of system security plans and threat and risk assessments given how few have been prepared.
- Audit did not find evidence of a plan to manage the risks of not classifying electronic documents. Shared Services ICT relies on an informal system, such as promotion of business rules, and training to manage risks. Additional layers of electronic security are also applied to data when requested.
- Security clearances of staff complement the classification of documents and other electronic and physical controls over information as part of a wider protective security framework to manage the risk associated with sensitive information. The security level of data storage, either physical or electronic, is determined by the relative sensitivity or risk associated with the information. Security clearances to the appropriate level are required for staff to access classified information.
- Obtaining a security clearance carries with it a cost as well as a time commitment, with higher level security clearances being relatively more expensive and time consuming to obtain. Clearances for non-Australian citizens add an additional factor to the usual clearance process, and can at

times be considerably more time-consuming to obtain. This is a particular factor as employment within the ACT Government does not require Australian citizenship.

- Some Shared Services staff are located in directorates and agencies. There is no policy or obligation for these on-site teams to promote information and ICT security.
- There is a need for an electronic records management system. Such a system would require classification of electronic data, and specification of who may access it. Currently, there are no plans to introduce such a system for ACT Government directorates and agencies.
- The Government Information Office does not have a major role in information security, as do similarly named offices in other jurisdictions. However, given its broad strategic role, communication between this Office and other areas that are directly accountable for protective, information and ICT security, is important.

RECOMMENDATIONS AND RESPONSE TO THE REPORT

1.16 The audit made three recommendations to address the findings represented in this report. Priority should be given to the implementation of **Recommendation 1 a), Recommendation 2 b)** and **Recommendations 3 b), d), e) and g).**

1.17 In accordance with Section 18 of the *Auditor-General Act 1996*, a final draft of this report was provided to the Director-Generals of the Treasury and of Justice and Community Safety; the Executive Director, Shared Services Division for consideration and comments. Responses are as follows.

Response from the Director of Territory Records

In anticipating the need for agencies to address the requirements for an enhanced level of security in relation to the management of their records, the Territory Records Office is currently reviewing the Standard and Guideline for Records Management Number 1 – *Records Management Programs* to require agencies to reflect the application of the ACT security classification scheme and to integrate this into all aspects of their records management.

Response from the Director-General, Justice and Community Safety Directorate

The Justice and Community Safety Directorate notes that the objective of this audit was modified during the course of the audit. Assessment of whether the ACT Government has suitable systems and frameworks in place to ensure efficient and effective safeguarding of personal or sensitive information involves examination of governance arrangements, systems architecture and controls, and staff behaviour. While field work and focus was initially intended to include understanding InTACT (now Shared Services ICT) roles and

responsibilities, as both an ICT policy area and service provider, and the way this works in practice with agencies, Justice and Community Safety Directorate acknowledges that it would be difficult to draw meaningful conclusions from testing only a sample of systems and staff behaviours.

In the circumstances it may be premature for Audit to conclude that it is unclear whether the status of the *Protective Security Policy and Guidelines* is well understood by agencies or whether they are complying with it. Nevertheless Justice and Community Safety will, through its leadership of the ACT Security in Government Committee, work collaboratively with other agencies to ensure good governance in this area as the ACT Government makes adjustments to its protective security framework in light of changes at the Commonwealth level.

1.18 In addition, the Directors-General provided responses to each recommendation, as shown below.

Recommendation 1 - Shared Services Division and Justice and Community Safety Directorates should improve whole-of-government security management practices by:

a) clarifying and documenting the roles and responsibilities of an ACT Government IT Security Advisor, the ACT Security in Government Committee and directorate Agency Security Advisors and their supporting communication processes. Directorates and agencies should be given information on these roles and responsibilities and communication processes once clarified (high priority); and

b) formalising the relationship between Security and Emergency Management Branch, and Shared Services ICT Security Section.

Response from the Director-General of Justice and Community Safety Directorate

Agreed.

The Justice and Community Safety Directorate agrees that clarifying and documenting the various roles and responsibilities will be of assistance to all directorates in the management of information security. This will also formalise the relationship between the Justice and Community Safety Directorate's Security and Emergency Management Branch and Treasury Directorate's Shared Services ICT Security Section.

Response from the Under Treasurer (Shared Services)

Part a) – Agreed

Roles and responsibilities documents, and associated communication process information, will be prepared based on industry and Commonwealth best practices and

standards and will be communicated to directorates once complete. Target date: 1 January 2013.

Part b) – Agreed

Discussions will commence as soon as possible with Security and Emergency Management Branch, Justice and Community Safety Directorate on the governance required to support the formalisation of the relationship. Shared Services recommends formalisation of the arrangement in the new revision of the *Protective Security Policy and Guidelines.* Target date: 1 October 2012.

Recommendation 2 – The Justice and Community Safety Directorate through its leadership of the ACT Security in Government Committee, should improve whole-of-government security management practices by:

a) establishing a process for surveying and reporting on compliance by directorates with approved information security policy, procedures and guidance material and using the results to inform review of these documents as required;

b) completing the review of the *Protective Security Policy and Guidelines* and in so doing:

- **continue working to clarify which of the Commonwealth's 33 mandatory requirements for protective security, including information security, will be mandatory for ACT directorates and agencies;**
- **include references to international standards on information and ICT security (high priority);**

c) addressing in its risk plan that not keeping information security policy and procedure current will restrict agencies ability to meet their information security obligations;

d) encouraging all directorates to include in their risk plans the risk of not being compliant with information security obligations and guidance; and

e) completing the current review of the operations of the ACT Security in Government Committee in relation to information security management.

Response from the Director-General of Justice and Community Safety Directorate

Agreed.

On 23 May 2012 the Security and Emergency Management Senior Officials Group accepted revised terms of reference for the ACT Security in Government Committee, following a review by the ACT Security in Government Committee. These revised terms of reference will include the role of 'reviewing and updating the ACT *Protective Security*

Policy and Guidelines' and a requirement to 'provide an annual report to the Security and Emergency Management Senior Officials Group on agencies' compliance with the *Protective Security Policy and Guidelines'.* The ACT Security in Government Committee will use this information to review information security documents as required.

Review of the *Protective Security Policy and Guidelines* has already commenced and will include clarification of which of the Commonwealth's 33 mandatory requirements for protective security will be mandatory for ACT directorates and agencies and references to international standards on information and ICT security.

The Justice and Community Safety Directorate will add to its risk management plan the risk of not keeping information security policy and procedures current. The Justice and Community Safety Directorate will encourage all directorates to include in their risk plans the risk of not being compliant with information security obligations and guidance.

Response from the Under Treasurer (Shared Services)

Part a) – Agreed

Shared Services will work collaboratively with Security and Emergency Management Branch on this issue.

Parts b) through e) - Agreed

Recommendation 3 - Shared Services Division should improve whole-of-government security management practices by:

a) advising directorates and agencies acquiring information services from private suppliers on potential security issues that may compromise the ACT Government's information security standards;

b) sponsoring the development of a mandatory requirement that:

- **in general all directorates' and agencies' websites are hosted on the ACT Government network or by an ACT Government endorsed supplier; or**
- **where web applications are deployed on external hosts they should meet acceptable security, governance and change management standards; and**
- **web based applications that are not meeting acceptable security, governance and change management standards must be remediated or removed (high priority);**

c) referencing international information and ICT security standards in key information security documents;

d) developing whole-of-government policies and procedures for managing ICT security in relation to new technologies, particularly for portable platforms (high priority);

e) fostering a mandatory requirement that directorates and agencies develop system security plans, and threat and risk assessments for:

- **all new ICT systems; and**
- **legacy ICT systems using a risk analysis (high priority).**

f) directing on-site teams to promote information and ICT security as part of their routine activities; and

g) planning for an ACT Government electronic records management system and pursuing funding for its implementation (high priority).

Response from the Director-General of Justice and Community Safety Directorate

Noted.

While this recommendation is targeted at the Shared Services Division for implementation, the Justice and Community Safety Directorate will work with Shared Services where applicable to ensure progress.

Response from the Under Treasurer (Shared Services)

Part a) – Agreed.

Shared Services will ensure that processes are in place to communicate security issues and risk information to directorates for all external procurement activities.

Part b) all – Agreed

Shared Services will work collaboratively with Security and Emergency Management Branch to develop the policy, which will then be presented to the Information Strategy Committee to endorsement. The draft policy will include seeking endorsement for the website hosting requirements to become mandatory. The policy approach is expected to be flexible and scaleable to ensure that website hosting costs does not become unnecessarily costly, and that comparatively low through high sensitivity levels of information are catered for in an appropriate way. Target date: 1 January 2013.

Part c) – Agreed

New documents will include the applicable references and existing documentation will be amended. Target date: 1 January 2013.

Part d) – Agreed.

A significant body of work on policy, protocols and procedures relating to mobile technology has already been undertaken and is close to completion. Target date: 1 October 2012.

Part e) – Agreed.

Shared Services will communicate this requirement for all new ICT systems, based on their associated risk profiles, and incorporate it as part of the project proposal phase of the system implementation as necessary. Target date: 1 October 2012.

For legacy systems, the level of workload within this requirement will necessitate a prioritisation of effort. Shared Services agrees that high priority and critical systems, with a medium to long-term remaining lifecycle, should be selected for early analysis. Shared Services is also able to manage the process at a whole-of-government level and provide assistance to directorates to achieve assessments for those systems. Target date: 1 December 2012 (for identification of systems requiring immediate assessment).

Part f) - Agreed

Part g) – Agreed.

Shared Services will work with the Territory Records Office to ensure that any whole-of-government electronic records management system has both the capabilities and security controls appropriate for the ACT Government computing environment.

Options to improve record keeping, security and provide better collaboration for directorates through electronic records management (within available funding) will be examined. Target date: 30 November 2012.

ACKNOWLEDGEMENTS

1.19 The Auditor-General's Office acknowledges the co-operation and assistance of the management and staff of:

- the Justice and Community Safety Directorate;
- Treasury Directorate - Shared Services Division;
- Chief Minister and Cabinet Directorate;

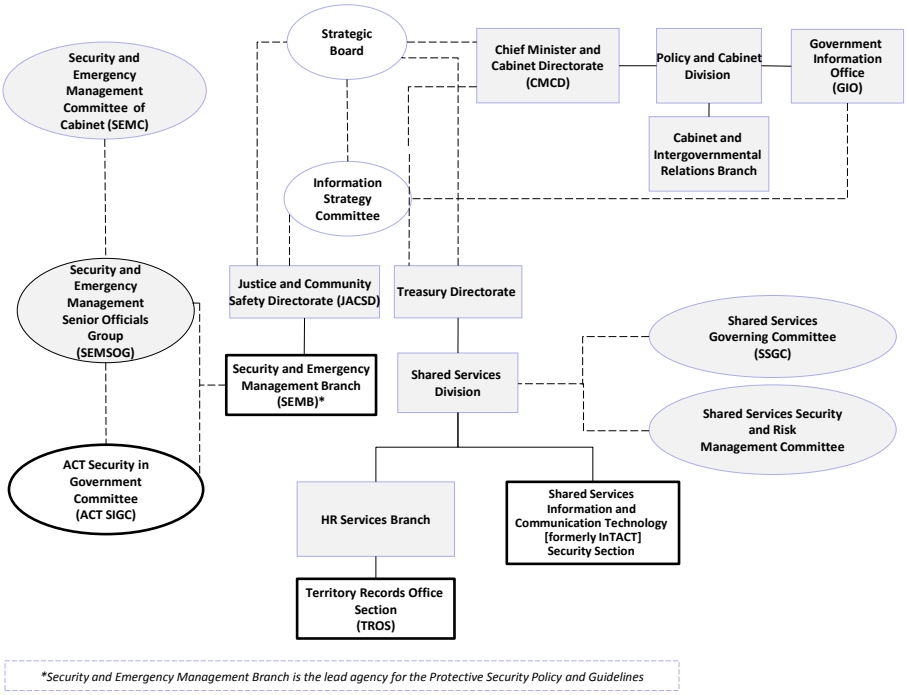
in the production of this report. The Office also acknowledges the assistance of Mr Graham Smith of Numerical Advantage Pty Ltd, and Mr Lee Mansfield of Oakton Ltd.

2. WHOLE-OF-GOVERNMENT INFORMATION AND ICT SECURITY MANAGEMENT AND SERVICES

RESPONSIBILITIES

2.1 The whole-of-government administrative structure for protection, information and ICT security is shown in Figure 1. Those areas with key functions have bolded borders.

Figure 1: Whole-of-government protective, information and ICT security administrative structure



Source: Audit Office

2.2 Responsibility for whole-of-government protective, information and ICT security management and services primarily resides with:

- from a policy perspective with:
  - Justice and Community Safety Directorate's Security and Emergency Management Branch (SEMB) which is responsible for managing the ACT Government's protective security policy and documentation, and supporting key security and emergency management committees;
  - Treasury Directorate's Territory Records Office which administers the Territory Records Act;

- from a management of technology perspective with Treasury Directorate's Shared Services Division's, Shared Services ICT Security Section which is the ACT Government's Information and communication technology provider; and
- from an operational perspective each directorate and agency (not shown in Figure 1) are responsible for ensuring policies and procedures are in place so that staff comply with whole-of-government policies in managing their ICT.

2.3 Chief Minister and Cabinet Directorate's Cabinet and Intergovernmental Relations Branch maintain the *Cabinet Handbook,* which sets standards for the storage, distribution and classification of Cabinet documents.

2.4 Within Chief Minister and Cabinet Directorate there is also a Government Information Office. Government Information Offices in other jurisdictions manage information security but in the ACT this is not one of its functions.

2.5 The Senior Manager of Shared Services ICT Security Section is designated as the ACT Government's Information Technology Security Advisor by the Shared Services Governing Committee, and accepted as such by the ACT Security in Government Committee.

2.6 The duty statement for the role of the ACT Government Information Technology Security Advisor is found in the *ICT Security Policy.* The Security Advisor's duties are to:

- undertake compliance audits across the ACT Government in accordance with the agreed ICT/Information Security audit program;
- provide reports to the security executive on compliance across the ACT government;
- conduct duly authorised investigations into ICT/Information Security and policy compliance incidents; and
- provide assistance to authorised officers in the conduct of criminal and administrative investigations.

2.7 Accordingly, this is a particularly important role with respect to ICT security.

2.8 The appointment of a security advisor did not appear to have lead to better access to agencies on ICT security matters, possibly because this role is not widely known or understood across all directorates. This is a particularly important role with respect to ICT security and should therefore be promoted across all directorates and agencies.

2.9 Security and Emergency Management Branch staff regarded Shared Services ICT Security Section's contribution as technical, although some Shared Services ICT

policy is management and procedure, rather than technical. In turn, Shared Services ICT staff consider the Security and Emergency Management Branch's role as concerned with physical and personnel, not ICT security.

2.10 While there is a strong informal relationship between the Security and Emergency Management Branch and Shared Services ICT this could change with changes in staff. Accordingly it would be prudent to formalise this relationship.

2.11 Various committees and a board, shown in Figure 1 at page 17, have a role in protective, information and ICT security. For the purposes of this Audit the three committees that are of particular importance are the Security and Emergency Management Senior Officials Group, ACT Security in Government Committee and the Information Strategy Committee. The Information Strategy Committee reports to the Strategic Board.

2.12 Amongst its other functions, the Information Strategy Committee:

- has direct oversight of strategic 'One Government' Information Projects; and
- advises the Strategic Board on broad strategic priorities.

2.13 The function of the ACT Security in Government Committee is to:

> develop, implement, and review matters relating to protective security across government…

2.14 The Information Strategy Committee's 'One Government' Information Projects and ICT priorities, and the ACT Security in Government Committee's role in protective security across government, could all affect information security matters.

2.15 The ACT Security in Government Committee advises and reports to the Security and Emergency Management Senior Officials Group. There is a need to clarify the role of these committees in relation to whole-of-government information security matters.

2.16 The inter-relationships and communication between committees co-ordinated within directorates is defined. However, with respect to the Information Strategy Committee and the ACT Security in Government Committee, which are co-ordinated by different directorates, it is not clear how these interact to share information.

2.17 Overall, whole-of-government information security roles and responsibilities and communication processes are not well defined and documented. Such information should be readily available.

2.18 Given the above and the importance of information security it is timely for information security roles, responsibilities and communication processes to be

clarified. Once this is completed all directorates and agencies should be given information on their roles, responsibilities and communication processes. Such information should be kept up to date.

Recommendation 1 - Shared Services Division and Justice and Community Safety Directorate should improve whole-of-government security management practices by:

a) clarifying and documenting the roles and responsibilities of an ACT Government IT Security Advisor, the ACT Security in Government Committee and directorate Agency Security Advisors and their supporting communication processes. Directorates and agencies should be given information on these roles and responsibilities and communication processes once clarified (high priority); and

b) formalising the relationship between Security and Emergency Management Branch, and Shared Services ICT Security Section.

JUSTICE AND COMMUNITY SAFETY DIRECTORATE

Security and Emergency Management Branch

2.19 The Security and Emergency Management Branch (SEMB) provides whole-of-government strategic policy advice on protective security, counter terrorism, critical infrastructure protection and emergency management issues. It is the lead policy agency for protective security in the ACT Government.

2.20 Inter alia, the Security and Emergency Management Branch is responsible for 'creating a security culture across ACT Government through protective security policy and education'. It is the custodian of the ACT's *Protective Security Policy and Guidelines*, the latest edition of which was issued in October 2007. The *Protective Security Policy and Guidelines* is supplemented by a *Security Awareness Handbook*.

2.21 While Shared Services ICT (formerly InTACT) Security Section and the Territory Records Office publish guidelines for information classification, these guidelines pay due regard to the *Protective Security Policy and Guidelines* and intend to be consistent with it.

The Protective Security Policy and Guidelines

2.22 The *Protective Security Policy and Guidelines* is based on the Commonwealth's former *Protective Security Manual.* The *Protective Security Policy and Guidelines* contains approximately 32 pages on information security in Section 3.

2.23 The *Protective Security Policy and Guidelines* is currently under review. The ACT Security in Government Committee will make a recommendation to the Security and Emergency Management Senior Officials' Group by December 2012 . At an

unspecified time later the Senior Officials' Group will make a recommendation on a revised manual to the Security and Emergency Management Committee of Cabinet.

2.24 Importantly, the *Protective Security Policy and Guidelines* states that information security is the responsibility of directorates and agencies, not the Shared Services ICT Security Section or another external service provider. The Government expects agencies to identify valuable and sensitive information through sound risk assessment and to ensure that it is protected from compromise or misuse.[3]

2.25 International Standard AS/NZS ISO/IEC 27001:2006 *Information technology – security requirements – information security management systems – requirements* are not referenced in the *Protective Security Policy and Guidelines.*

2.26 As discussed later in this report (see paragraphs 2.79 to 2.84) the international standards are integrated into the Commonwealth's *Protective Security Policy Framework* as reference material. The *Protective Security Policy Framework*'s mandatory requirements for information security are drawn from the Commonwealth's Defence Signals Directorate's *Information Security Manual,* which is a leading authority on information security.

2.27 Audit considers that international standards on information and ICT security management should be referenced in the revised *Protective Security Policy and Guidelines*, to assist directorates and agencies in managing information security.

2.28 The *Protective Security Policy and Guidelines,* the pre-eminent protective security document for the ACT Government, states that '…standards, while not mandatory, will assist in the transition to a security culture within the ACT Government' and also states directorates and agencies 'should' and even 'must' do certain things. This ambiguity is being addressed in the review underway of this document. As part of the revision of the *Protective Security Policy and Guidelines*, the Security and Emergency Management Branch prepared an options paper for the ACT Security in Government Committee meeting of June 2011 to discuss which of the 33 mandatory protective security requirements in the Commonwealth's *Protective Security Policy Framework* are applicable to the ACT.

2.29 It is in the ACT Government's interests that agencies comply with mandatory requirements in the *Protective Security Policy and Guidelines*. Attention paid to it will assist greatly in efforts to promote it as part of a security culture across all government directorates and agencies.

[3] ACT *Protective Security Manual and Guidelines,* paragraphs 1.2.3 (page 4), and 3.1.7 (page 37)

2.30 The ACT Security in Government Committee's terms of reference require it to report annually to the Security and Emergency Management Committee of Cabinet, via the Security and Emergency Management Senior Officials Group on the status of protective security across all government agencies. To this end, it has reported to the Security and Emergency Management Senior Officials Group seven times since November 2007.

2.31 Acting on the advice of the ACT Security in Government Committee, the Security and Emergency Management Branch surveyed agencies in April 2008 to 'set a benchmark of security risk management procedures …, identify gaps and areas of improvement, and implement … mitigation measures'. The information security questions covered information security advice and directives found in the *Protective Security Policy and Guidelines* and the subsequent report was submitted to the Security and Emergency Management Executive Committee (the predecessor to the Security and Emergency Management Senior Officers Group) in November 2008. The Committee endorsed the report's submission to the Security and Emergency Management Committee of Cabinet.

2.32 The ACT Security in Government Committee reported on agency progress in implementing the 24 recommendations of the report to the Security and Emergency Management Committee of Cabinet meeting of October 2009. Subsequently, that Committee issued to the full Cabinet its first annual report on progress against all 24 recommendations. One of the recommendations was marked as completed at the time of this first progress update, and a further five recommendations were ongoing in nature. However, no further reports of progress were produced.

2.33 A recommendation of the initial report to Cabinet was for electronic surveys of protective security to be conducted every two years. The ACT Security in Government Committee meeting on February 2009 noted this recommendation. However, it has not been acted upon.

2.34 Audit concludes that SEMB, the ACT Security in Government Committee and the Security and Emergency Management Senior Officers Group do not have current information on compliance with the *Protective Security Policy and Guidelines* across all directorates. The current state of compliance with protective security requirements across the ACT Government is undocumented, and the risk of security gaps being unnoticed and uncontrolled is therefore increased.

2.35 The ACT Security in Government Committee proposes that in the future information on Directorates' and agencies' compliance with the *Protective Security Policy and Guidelines*, is reported annually to the Security and Emergency Management Senior Officials Group.

2.36 Information on compliance could assist Agency Security Advisors (see paragraphs 2.43 to 2.50) in all directorates and agencies in promoting information security.

Recommendation 2 - The Justice and Community Safety Directorate through its leadership of the ACT Security in Government Committee, should improve whole-of-government security management practices by:

a) establishing a process for surveying and reporting on compliance by directorates with approved information security policy, procedures and guidance material and using the results to inform review of these documents as required.

2.37 The *Protective Security Policy and Guidelines* was modelled on the Commonwealth's *Protective Security Manual*. In June 2010, the Commonwealth replaced the *Protective Security Manual* with the *Protective Security Policy Framework*.

2.38 The *Protective Security Policy Framework*, like its predecessor the *Protective Security Manual*, is the primary protective security document in the Commonwealth. There are 33 high level mandatory requirements in the *Protective Security Policy Framework*, compared to the *Protective Security Manual's* 400 plus minimum standards. The *Protective Security Policy Framework* relies on agencies' undertaking a security risk assessment and considering information that includes Australian Government guidelines, international information and ICT standards, and better practice publications to determine their security controls.

2.39 Some of the major changes advanced through the *Protective Security Policy Framework* include:

- Security classification levels were changed. Levels are now Protected, Confidential, Secret and Top Secret;
- The introduction of Dissemination Limiting Markers, to replace x-in-confidence caveat and restricted classification level, allows agencies to better manage their business as usual information;
- The majority of the *Protective Security Policy Framework* is a public document; however access to some parts is restricted. (The former *Protective Security Manual* was not a public document);
- The *Protective Security Policy Framework* shifts the focus from document handling to information security management in the modern digital world; and
- The *Protective Security Policy Framework* requires agencies to annually report their compliance with the mandatory requirements to their respective portfolio Minister.

2.40 The *Protective Security Policy and Guidelines* are currently being reviewed, and in so doing the Commonwealth's *Protective Security Policy Framework* and ACT directorates and agencies business needs will shape the revised document.

2.41 The ACT Security in Government Committee has adopted the new classification system of the Commonwealth's *Protective Security Policy Framework* (Protected, Confidential, Secret and Top Secret). At its 8 February 2011 ACT Security in Government Committee agreed that:

> pending sign off from the Commonwealth Attorney-General, a recommendation will be made to the Security and Emergency Management Senior Officers' Group regarding the adoption of the Commonwealth classification system.
>
> Further work is required on which of the 33 mandatory requirements should be adopted by the ACT Government.

2.42 The ACT Security in Government Committee is reviewing *Protective Security Policy and Guidelines*. The Committee intends to recommend to the Security and Emergency Management Senior Officers' Group the adoption of a subset of the 33 mandatory requirements. It is proposed that the revision of the *Protective Security Policy and Guidelines* be considered by the ACT Security in Government Committee by December 2012, and at an unspecified time later, by the Security and Emergency Management Senior Officers' Group. The Security and Emergency Management Committee of Cabinet will approve the revised Protective Security Policy and Guidelines following the Security and Emergency Management Senior Officers' Group's review.

Recommendation 2 – The Justice and Community Safety Directorate through its leadership of the ACT Security in Government Committee, should improve whole-of-government security management practices by:

b) completing the review of the Protective Security Policy and Guidelines and in so doing:

- **continue working to clarify which of the Commonwealth's 33 mandatory requirements for protective security, including information security, will be mandatory for ACT directorates and agencies; and**
- **include references to international standards on information and ICT security (high priority).**

Creating a security culture

2.43 The Security and Emergency Management Branch is the branch responsible for creating (meaning promoting and facilitating) a security culture across ACT Government directorates. Awareness of protective security and information

security amongst employees is the purpose of the Security and Emergency Management Branch's *Security Awareness Handbook.*

2.44 Key personnel in creating a security culture within directorates and agencies are the Agency Security Advisors. It is also important to have an executive security 'champion'.

2.45 Agency Security Advisors are senior officers who are responsible for providing advice on security risk and helping managers and employees devise and implement appropriate physical, personnel and *information security* measures and plans (emphasis added).[4]

2.46 They assist in the ongoing implementation of measures outlined in the *Protective Security Policy and Guidelines* and 'play key roles in conducting the agency's security risk assessment and preparing the agency's security policy and plan'[5].

2.47 Importantly, Agency Security Advisors should 'liaise as appropriate with relevant agencies, for example Shared Services ICT, in determining appropriate information technology communication security'[6]. The matter of communication between Shared Services ICT and agencies is discussed later in this report (see paragraph 2.112).

Risk management

2.48 The Justice and Community Safety Directorate's *Business Risk Management Plan* records as 'high' a risk of 'ineffective oversight of the protective security arrangements across the Territory and within JACSD' because this event is unlikely, but will have major (unspecified) impacts. To treat this risk, Justice and Community Safety Directorate issued the *Protective Security Policy and Guidelines*. The resulting residual risk, after this risk treatment, is judged to be low.

2.49 Issuing the *Protective Security Policy and Guidelines* with amendments is not the same as actively promoting its use and monitoring compliance with it. Audit considers that action to monitor compliance with the *Protective Security Policy and Guidelines* is lacking (see paragraph 2.34), and therefore the major impacts of non compliance referred to in the risk plan have a greater chance of being realised.

2.50 Furthermore, while it is a role of the Security and Emergency Management Branch to create a security culture through promotion of the protective security

[4] ACT *Protective Security Manual and Guidelines,* paragraph 1.2.10

[5] ACT *Protective Security Manual and Guidelines*, paragraph 1.2.8, p. 5

[6] ACT *Protective Security Manual and Guidelines*, paragraph 1.2.8, p. 5

framework to directorate and agencies, the Directorate's risk plan does not address risks related to this. A major task of the Security and Emergency Management Branch in managing this risk is to issue and to update information security policy and procedure, and to ensure that directorates acknowledge this risk.

Recommendation 2 - The Justice and Community Safety Directorate through its leadership of the ACT Security in Government Committee, should improve whole-of-government security management practices by:

c) addressing in its risk plan that not keeping information security policy and procedure current will restrict agencies ability to meet their information security obligations; and

d) encouraging all directorates to include in their risk plans the risk of not being compliant with information security obligations and guidance.

Support for the Security and Emergency Management Committees of Government

2.51 As shown in Figure 1 at page 17, the Security and Emergency Management Branch supports, through secretariat services and/or the provision of information, a hierarchy of government committees dedicated to security in general.

- The Security and Emergency Management Senior Officials Group that in turn supports the Security and Emergency Management Committee of Cabinet by providing strategic policy advice on protective security, counter terrorism and emergency management. It is chaired by the Director-General of JACSD, and its membership is legislated by the ACT *Emergencies Act 2004,* section 142.
- Security and Emergency Management Planning Group that develops, implements and reviews specific security and emergency management matters including plans and sub-plans, reporting to the Security and Emergency Management Senior Officers' Group.
- Closed Circuit Television Working Group facilitates and monitors the progress of the Government's review of CCTV capability in the ACT.
- The ACT Security in Government Committee's role is to:

  ... develop, implement and review matters relating to protective security across government, including the implementation of the ACT Protective Security Training Framework across agencies.
- The ACT Security in Government Committee is chaired by the Deputy Director-General, Community Safety in JACSD, and is made up of Agency Security Advisors and Agency Security Officers from each directorate.

The ACT Security in Government Committee

2.52 The terms of reference of the ACT Security in Government Committee are:

> to develop, implement and review matters relating to protective security across government …[7]

2.53 In relation to the operation of the ACT Security in Government Committee, Audit found that:

- In accordance with its terms of reference, the Committee has met approximately twice a year since March 2007.
- Documents drafted by the Treasury Directorate's Shared Services and Information Communication and Technology Security Section are noted by the ACT Security in Government Committee, rather than approved or adopted by it. The Committee has no formal role in reviewing or co-ordinating Shared Services ICT's activities in issuing policy or procedures for information security management, despite having focus in this area;
- At its February 2009 meeting the ACT Security in Government Committee agreed to the establishment of an Information Security Working Group. The proposal lapsed when the sponsoring agency, the Territory and Municipal Services Directorate (through the Territory Records Office), withdrew support for it. Audit could not determine if the rationale for such a Group had similarly lapsed.
- The Committee's Terms of Reference require it to implement the ACT Protective Security Training Framework. The Committee implemented the Framework for 2009-10, but not subsequently. The Security and Emergency Management Branch advised that the Committee has since developed guidelines to support Agency Security Advisors in implementing protective security policy and procedure.
- The Committee resolved at its September 2009 meeting to issue a security newsletter. Only one edition of the newsletter was produced. Production of the newsletter was the responsibility of the Security and Emergency Management Branch, which did not resource its continuation. Instead, to communicate with members of the Committee, the Security and Emergency Management Branch currently posts information to a sharepoint site.
- The minutes of the ACT Security in Government Committee meetings from February 2009 to June 2011 do not reference any discussion of compliance with the *Protective Security Policy and Guidelines*, although it is a topic of direct relevance to the Committee. The Security and Emergency

[7] Terms of Reference, ACT Security in Government Committee

Management Branch advised that some topics discussed during this time implicitly involved discussion of compliance. At its April 2012 meeting the Committee discussed this topic.

2.54 The ACT Security in Government Committee needs to meet its terms of reference or its operations need to be clarified. This can be achieved in the current review of its operations.

Recommendation 2 - The Justice and Community Safety Directorate through its leadership of the ACT Security in Government Committee, should improve whole-of-government security management practices by:

e) completing the current review of the operations of the ACT Security in Government Committee in relation to information security management.

Information classification

2.55 The system security plan referred to in paragraph 2.89 relies on a risk assessment of the data that is to be stored. Such a risk assessment is required by the system security plan template to address data usability, cost of controls and security measures. For example, where an agency has accepted the risk attending broader access to sensitive data, tight controls over it would be unnecessary and unacceptable.

2.56 Shared Services ICT implements controls commensurate with those assessed risks, when requested to do so by the system manager.

2.57 As previously mentioned (see section The Protective Security Policy and Guidelines, page 20) the *Protective Security Policy and Guidelines* is under review. Currently, it requires hard copy and electronic data to be classified according to its risk. There are 3 levels of security classification for non-national security classifications, which are the majority of information held by ACT directorates. These classifications are highly protected, protected or x-in-confidence.

2.58 Audit found that there was some confusion regarding security classifications. A security classification is a response to the question: 'What damage will result from the release of this information?' The x-in-confidence caveat, examples being cabinet-in-confidence and security-in-confidence answers the question 'who should see this document?' Data security on ACT Government networks was not compromised by disagreements on whether x-in-confidence is a security classification or a caveat on who should see a document.

2.59 Under a proposal accepted by the Security and Emergency Management Senior Officials Group in February 2012, the ACT will adopt the Commonwealth's national security classifications of top secret, secret, confidential and protected.

In addition, information may have dissemination limiting markers attached to it. These will replace the x-in-confidence caveat and restricted classification markings on documents.

TREASURY DIRECTORATE

Shared Services ICT (formerly InTACT) Security Section

2.60 Shared Services ICT has these roles:

- supplier of information and communication technology goods and services;
- planner and strategist for whole-of-government information and communication technology; and
- minder of agencies information and communication technology, and in so doing to alert management to any risks.

2.61 Shared Services ICT was formed in 1996 as a shared ICT service created from the amalgamation and rationalisation of the ICT services within agencies. However, some services remained in directorates and agencies. For some staff, the transfer to Shared Services ICT was only one of form: they joined on-site teams in their former agency, overseeing the same or similar systems.

2.62 Shared Services ICT networks support 37 500 students and 5 000 teachers, 18 000 public servants and CIT students locally and overseas.

Shared responsibility for delivery of ICT services with directorates

2.63 ICT is fundamental to ACT Government directorates' operations. Foundational corporate planning and governance documents, such as Strategic Plans and Risk Management Plans, should acknowledge this.

2.64 Shared Services ICT's vision and purpose is presented in the *ICT Governance Statement* of November 2009 Inter alia, Shared Services ICT aims to be a 'trusted partner' to ACT Government directorates and agencies in delivering 'reliable, responsive, efficient and effective ICT services to the ACT Government'. Its goals include building 'effective working relationships'.

2.65 Shared Services ICT's policy documents require agencies to prepare and use:

- a Business Continuity Plan for each system;
- a Strategic Plan for agency business systems;
- System Security Plans;
- Incident Reporting Procedures;
- Threat and Risk Assessments;, and
- in the context of ICT projects, Business Plans and Risk Management Plans.

2.66 Most, but not all, agencies have service agreements with Shared Services ICT. Like all written agreements, service agreements regularise relations between client and service provider. Other agreements are specific to systems or projects, and support the general service level agreement.

2.67 Services provided by Shared Services ICT according to the service level agreement template include:

- Support and Maintenance - initial service requests or incident determination and tracking to achieve resolution of requests;
- Computing - computing services that enable employees to do their jobs productively. This includes security services;
- Communications - communication related services from telephone to full call centre infrastructures;
- Business Systems, such as business system and application development; and
- Planning and consulting. This service includes agreement management, ICT consulting and business services and project management.

2.68 The Shared Services model under which Shared Services ICT operates intends that service delivery should be shared, with mutual responsibilities. The standard service level agreement template includes the responsibilities of each party. Details of these responsibilities are expanded in the document *Statement of Responsibilities for ICT Service.*[8]

2.69 The Service Agreement template includes the following performance information items:

- monthly reports on service performance for incident response and resolution times are available via the ICT Manager. Reporting against these activities is reliant on all cases being logged;
- a service to monitor and report on service availability and performance measures. These have been in development since the release of the template, but have not been completed.

2.70 Agencies' responsibilities are to:

- fund any security-related upgrades to its business systems;
- ensure business practices and business system administration processes do not compromise security. (Shared Services ICT may monitor activities and raise security issues as necessary); and

[8] Latest version is dated November 2009.

- Business Continuity Planning, Disaster Recovery and Threat and Risk Assessments.

2.71 Some directorates and agencies use ICT services procured from the market, due to perceived cost and/or implementation timeline benefits, rather than Shared Services ICT despite it being the Government's designated supplier. Centralised services are likely to afford a higher level of overall security in relation to information security. Given this, an assessment is needed on the degree to which services secured from private suppliers may compromise information security and strategies should be developed to ensure that ICT security is protected.

2.72 The *Statement of Responsibilities for ICT Service* places the responsibility for data security with agencies.[9] There is a good reason for this - directorates own the data, know the information content, and therefore have the biggest interest in data security. This is also consistent with the *Protective Security Policy and Guidelines*, that regards information security as an agency responsibility.[10]

Recommendation 3 - Shared Services Division should improve whole-of-government security management practices by:

a) advising directorates and agencies acquiring information services from private suppliers on potential security issues that may compromise the ACT Government's information security standards.

Security incidents and metrics

2.73 Shared Services ICT Security Section maintains security metrics on its portal, that is part of the Shared Services intranet. These metrics are related to its important task of securing the perimeter of the ACT's network and internet access.

2.74 Shared Services ICT Security does not keep metrics on individual security incidents. Most incidents are related to acceptable usage and human resources rather than technical security.

2.75 Some websites of directorates and agencies have been compromised; however all of these occurred on externally hosted sites, that is, those outside Shared Services ICT's perimeter security controls. No figures on the (small) number of externally hosted website compromises are available, although these compromises are reported to Shared Services ICT Security.

2.76 Compromises can be minimised by ensuring that all websites are hosted on the ACT Government network or are part of an endorsed ACT Government supplier

[9] *Statement of Responsibilities for ICT Service*, page 5

[10] *ACT Protective Security Policy and Guidelines*, paragraphs 1.2.3 and 3.1.7

so that Shared Services ICT Security Section can provide guidance on what is required to maintain ICT security.

2.77 Where external hosting is required, directorates and agencies should procure from Shared Services ICT approved service providers. Web applications deployed by these providers should meet acceptable security, governance and change management standards, or be removed.

Recommendation 3 - Shared Services Division should improve whole-of-government security management practices by

b) sponsoring the development of a mandatory requirement that:

- **in general all directorates' and agencies' websites are hosted on the ACT Government network or by an ACT Government endorsed supplier; or**
- **where web applications are deployed on external hosts they should meet acceptable security, governance and change management standards; and**
- **web based applications that are not meeting acceptable security, governance and change management standards must be remediated or removed (high priority).**

Risk management

2.78 Shared Services ICT relies on agencies to document the risks associated with their own data and systems through the use of system security plans. Shared Services ICT had planned to update its *ACT Government Shared Services ICT Risk Management Plan 2011 – 2014* by 30 September 2011. This has been delayed and a new target date is yet to be set.

Security policy

2.79 As a service to agencies, Shared Services ICT maintains a library of ICT security-related material on the Shared Services website. The main documents related to ICT security are the *ICT Security Policy* and the *Security Policy Services Guide*.[11] These documents are supplemented by smaller, specific policy documents.

2.80 ICT security policy is continually being developed by Shared Services ICT Security Section, such as that for social media sites and hand-held devices. However,

[11] These documents are available from http://sharedservices/actgovt/ICTpolicies.htm under the ICT Security tab.

Audit could not find evidence that such policies are formally endorsed at a high level that would allow promotion and adoption at a whole-of-government level.

2.81 The Commonwealth's Defence Signals Directorate's *Information Security Manual*[12]is the model for the *ICT Security Policy* and the *Security Policy Services Guide.* This manual was adopted because of its authority within the Commonwealth. The Commonwealth's *Protective Security Policy Framework* contains the *Information Security Manual* as the authority on ICT security management.

2.82 International Standard AS/NZS ISO /IEC 27001:2006 *Information technology – security requirements – information security management systems – requirements* referred to previously (see paragraph 2.25) is the international benchmark on information security. Similarly, the Information Assurance and Controls Association (ISACA), an international association devoted to ICT security and control, has promulgated a set of guidance materials for IT governance.[13]

2.83 The Commonwealth's July 2011 *Information Security Management Protocol* (part of the *Protective Security Policy Framework*) includes the international information security standards as a reference - the international standards 'amplify' the *Information Security Management Protocol*. The *Information Security Management Protocol*'s structure and controls align with the international standard ISO/IEC 27001:2006.

2.84 The Commonwealth's Defence Signals Directorate's *Information Security Manual* is authoritative under the Commonwealth's *Information Security Management Protocol* in all key operational security areas. Thus, the approach used by Shared Services ICT Security Section to ICT security policy is broadly in line with that of the Commonwealth. However, the absence of reference to the international standards is a departure from the Commonwealth's approach. Directorates and agencies knowledge of information and ICT security and compliance with better practice would be enhanced if there was a reference to these international standards in key information and ICT security documents.

[12] Department of Defence, Intelligence and Security, *Australian Government Information Security Manual,* November 2010

[13] The Information Assurance and Controls Association (ISACA) publishes COBIT (Control Objectives for Information and related Technology). Details are available on the Association's website.

Recommendation 3 - Shared Services Division should improve whole-of-government security management practices by:

c) referencing international information and ICT security standards in key information security documents.

Maintaining perimeter security

2.85 Security of the ACT Government's networks, and of data stored in them, is a key function of Shared Services ICT.

2.86 Shared Services ICT maintains the perimeter security of the ACT Government networks and their applications. This includes testing patches and new software. The owners of the data inside the network, that is, those in the directorates and agencies that create and maintain it, should control access to those who are authorised.

2.87 Shared Services ICT Security has deployed a robust security regime in the defence of the ACT Government's information assets. While continuous vigilance is necessary, the current installation has successfully defended over one million attempts to access the ACT Government's network in the nine month period to 31 March 2012.

2.88 Notwithstanding this, hand held devices, known as 'portable platforms' that can access the ACT Government networks and the internet are proliferating. Use of these devices has raised a number of questions, such as, who owns the data on a device provided to an employee. Shared Services ICT Security is drafting and amending policies to govern the use of these mobile devices and other emerging technologies. Audit agrees that this needs to be a priority.

2.89 Directorates and agencies are required under Shared Services ICT information security policy and procedure to prepare threat and risk assessments, and system security plans.[14]. A system security plan involves assessing the risks and threats to an information system. It involves undertaking a risk management analysis and record. According to the Shared Services ICT template:

> the system security plan is a commitment by the system manager to put in place adequate measures to avoid, eliminate or reduce risks to an information system.

2.90 The system manager is not defined, but it is probably the manager responsible for continuation and operation of the system. In many cases, system managers appear to be the leader of the Shared Services ICT on-site teams.

[14] *ICT Security Policy*, Section 13

2.91 The system security plan has a central role in implementing the risk management and security of directorates and agencies information systems.

2.92 After a system security plan is signed by the system manager and the systems administrator, it is submitted to Shared Services ICT Security for review and feedback. Shared Services ICT Security makes a recommendation regarding its approval to the nominated Executive responsible for ICT Security in the directorate or agency.

2.93 Shared Services ICT's system security plan template is well structured and wide ranging. Inter alia, it covers system description, security objectives, data description, users and customers, education and training, physical security and other relevant topics.

2.94 The plan is data-centric as it addresses the risks inherent in the data the system contains. The system manager needs to identify the value of the information, and the risks to it, to enable Shared Services ICT Security to implement controls such as access control lists, encryption and physically separate storage.

2.95 Notwithstanding, there is low compliance with it. Of the 1025 systems identified by Shared Services ICT, 47 or less than 5% have a security plan. Of these 47 assessments, 42 were completed prior to 2007, the latest being approved in April 2010.

2.96 Threat and risk assessments (TRAs) are likewise not prepared by directorates or agencies. Of the 1025 systems, 23 or 2.24% only have assessments. No new assessments have been reviewed by Shared Services ICT security since June, 2010.

2.97 It is not clear to Audit why there are so few security plans or threat and risk assessments. This may be a problem related to communication between Shared Services ICT and directorates and agencies, who own the data in the systems. There is great scope for expanding the use of system security plans and threat and risk assessments given how few have been prepared.

Recommendation 3 - Shared Services Division should improve whole-of-government security management practices by:

d) developing whole-of-government policies and procedures for managing information security in relation to new technologies, particularly for portable platforms (high priority); and

e) fostering a mandatory requirement that directorates and agencies develop system security plans, and threat and risk assessments for:

- **all new ICT systems; and**
- **legacy ICT systems using a risk analysis (high priority).**

Security classifying electronic data

2.98 The Territory Records Office Standard and Guideline number 6 on digital records mandates that digital records are to conform with all record keeping requirements, including classification. The Shared Services ICT Security's *ICT Security Policy* also reflects the *Protective Security Policy and Guidelines*' requirements for electronic data to be protected through classification.

2.99 Security and Emergency Management Branch and Shared Services ICT Security agree that technical protection of the network, including through consideration of such mechanisms as electronic document classification, and staff education and security vetting are required to effectively protect electronic information. Technical enhancements would promote compliance with international and local information security standards. All action would be subjected to a rigorous risk-based cost benefit analysis prior to implementation.

2.100 Guidance provided in the *Protective Security Policy and Guidelines* on information classification is oriented toward hard copy classification. Currently, there is no automated method to classify digital data that is held on network drives, such as the ubiquitous G drive. When data is printed on paper and filed it is then able to be classified.

2.101 Shared Services has considered the need for an Electronic Document Security Classification (including email) system. It has not recently sought budget funding for this item due to other priorities. There is a need for a system to ensure that the ACT Government classifies its information assets in accordance with the ACT Government's *Protective Security Policy and Guidelines*. Currently the government fails to comply with its own ministerially endorsed policy.

2.102 Audit did not find evidence of a plan to manage the risks of not classifying electronic documents. These risks include:

- failure to comply with the requirement to classify data in the *Protective Security Policy and Guidelines*, as stated above;
- damage to the reputation of agencies that release sensitive, personal or public safety information;
- compromise to the security of the ACT Government networks.

2.103 Shared Services ICT relies on informal systems, such as the promotion of business rules and training, to manage risks. Additional layers of electronic security are also applied to data when requested.

2.104 Security clearances of staff complement the classification of documents and other electronic and physical controls over information as part of a wider protective security framework to manage the risk associated with sensitive information. The security level of data storage, either physical or electronic, is determined by the relative sensitivity or risk associated with the information. Security clearances to the appropriate level are required for staff to access classified information.

2.105 Obtaining a security clearance carries with it a cost as well as a time commitment, with higher level security clearances being relatively more expensive and time consuming to obtain. Clearances for non-Australian citizens add an additional factor to the usual clearance process, and can at times be considerably more time-consuming to obtain. This is a particular factor as employment within the ACT Government does not require Australian citizenship.

Training of agency staff

2.106 When invited, Shared Services ICT provides presentations to directorates and on security matters. These presentations emphasise general areas of weakness in security management.

Audit functions

2.107 Using publicly available audit software tools, Shared Services ICT has identified significant problems in directorates' password setting practices. Results of its audits were previously on the Shared Services ICT Security's webpage.

Shared Services ICT Security Section relations with clients

2.108 Shared Services ICT Security relies on good communications with its client agencies to promote a security culture, ICT security policies and its other functions. As a small but strategically important section, it must rely on other sections of Shared Services ICT, directorate and agency security personnel, and whole-of-government committees to deliver its messages. As discussed below, Audit found there is an opportunity for on-site teams, in particular, to promote a security culture.

Shared Services ICT's on-site teams

2.109 Shared Services ICT maintains on-site teams in directorates. Staff are employed by Shared Services ICT, but are located in the offices of their client directorates.

2.110 As noted at paragraph 2.68, Audit observed that Shared Services ICT's role is expected to be that of a provider of services, rather than a partner with shared responsibilities. Shared Services ICT on-site's role is similar to that of an ICT section as if it were part of a directorate or agency. They do not actively promote Shared Services ICT information security policies, although they are responsive to requests for assistance from their client directorates.

2.111 There is no policy or obligation to promote information and ICT security by the Shared Services ICT on-site teams. These teams consult with Shared Services ICT Security only when required, although on-site teams contribute to security plans for new, but not necessarily existing, systems.

Recommendation 3 - Shared Services Division should improve whole-of-government security management practices by

f) directing on-site teams to promote information and ICT security as part of their routine activities.

Promotion of information security in agencies

2.112 Shared Services ICT Security have no right of entry into directories or agencies to promote ICT security, despite the fact the Senior Manager of Shared Services ICT Security is designated as the ACT Government's IT Security Advisor by the Shared Services Governing Committee, and accepted as such by the ACT Security in Government Committee.

2.113 The ACT Government IT Security Advisor was not informed of a theft of data from a directorate. There was a chance, although small, the data could have been used to identify clients of the directorate. The directorate did not involve the IT Security Advisor in resolving the situation, as the problem was 'non technical'. It also held the data belonging to the directorate which was responsible for its management.

2.114 If involved, the IT Security Advisor could have identified opportunities to prevent similar situations occurring in the future and disseminated this information to all directorates and agencies.

2.115 Where directorates and agencies have approached the IT Security Advisor for advice, Audit found that that person or other members of Shared Services ICT Security applied their expertise to assist. Shared Services ICT also conducts roadshows to promote ICT security when requested. These presentations cover

topics such as email, privacy, passwords, internet and physical security. The number of roadshows appears small given the number of directorates and agencies.

2.116 As stated in paragraph 2.45 the Agency Security Advisors role includes promotion of information security.[15] Audit did not find evidence to suggest they do this; the low take up of system security plans in agencies (paragraph 2.95) suggests that this is an issue.

Territory Records Office

2.117 The Territory Records Office is responsible for regulating records management in the ACT. Its primary legislation is *Territory Records Act 2002.* The Director of the Territory Records Office issues standards, guidelines and record advices on recordkeeping, including digital recordkeeping.[16].

2.118 Directorates must comply with the Territory Records Office's standards, guidelines and record advices. Recordkeeping standards are Notifiable Instruments issued under the *Territory Records Act 2002* and have legal authority.[17].Guidelines and records advices are not legal instruments, but are ACT Government recordkeeping policy. A full list of the Territory Records Office's standards and other material relevant to electronic recordkeeping is at Appendix C, page 49.

2.119 Under the *Territory Records Act 2002*:

> records are information created and kept, or received and kept, as evidence and information by a person in accordance with a legal obligation or in the course of conducting business; and includes information in written, electronic or any other form.

2.120 Consistent with findings in its previous audit of recordkeeping, *Records Management in ACT Government Agencies*[18], this audit found that some staff, including senior staff, distinguished records from information. For example, drafts would be excluded from recordkeeping systems as they were not records, but information.

2.121 Audit's view in its previous audit was that to distinguish between documented information and records is a distinction without a difference.

[15] ACT Government, *Protective Security Policy and Guidelines,* paragraph 1.2.8, p5

[16] Section 18, *Territory Records Act 1992*

[17] Territory Records Act 2002, section 18

[18] Report No.3 of 2008

2.122 Of particular relevance to this audit is the Standard for Records Management No. 6 *Digital Records*. The Audit Office in its 2008 report *Records Management in ACT Government Agencies* report observed that:

> The Territory Records Office's Standard for Records Manag*ement No. 6: D*igital Records and its accompanying gu*ideline contain substantial information on the* management of digital records but do not specifically dictate the criteria required for digital records to be considered legally valid.

2.123 The 2008 Audit recommended the TRO should:

> subject to legal advice, improve the Standard for Records Management No. 6 Digital Records to provide sufficient information for agencies to assess the legal validity of their digital records; assist agencies in assessing the suitability of electronic recordkeeping systems or tools ...; and assess the suitability of electronic recordkeeping systems or tools for wider application across government.[19]

2.124 This recommendation was agreed.

2.125 In March 2011, the Director of the Territory Records Office issued *Standard for Records Management Number 9: Records Digitisation and Conversion* Approval 2011 (No 1). This standard appears to overcome any barriers to the use of digital records as evidence, and removes the requirement for agencies to regard hard copy as the only records acceptable under the Act.

2.126 Supplementing the standards are guidelines and specific advices. The Territory Records Office Records Advice Number 4 *What is a Recordkeeping System* states that records management systems should identify the business activities to which a record relates and then link it to other records to facilitate description, control, retrieval, disposal and access; and assign rights or restrictions to use or manage particular records.

2.127 The 2008 Audit report stated that:

> In many smaller agencies, or those without a need for a full electronic recordkeeping system, many digital business records were managed through means, such as shared network drives, that were not recognised record management systems or tools. These systems also catered for digital documents that could not be stored readily in agencies existing electronic systems.

2.128 Records Advice Number 4, *What is a Recordkeeping System* and the 2008 Audit, highlight the need for an electronic records management system. This need was reiterated by the Hawke report (see paragraph 2.135), and by a 2011 paper

[19] Recommendation 6 (Chapter 3) of the Office's *Records Management in ACT Government Agencies* performance audit report, tabled in June 2008.

commissioned by the Territory Records Office entitled *Digital Recordkeeping Pathway for Territory Records Office*[20].

2.129 Such a system would also require classification of digital data, and specification of who may access it. Currently, there are no plans to introduce such a system for ACT Government directorates and agencies. Given its importance, planning for its implementation should commence so that it can readily be deployed once funding is secured.

Recommendation 3- Shared Services Division should improve whole-of-government security management practices by

g) planning for an ACT Government electronic records management system and pursuing funding for its implementation (high priority).

APPROVAL OF DRAFT POLICIES, AND GENERAL OVERSIGHT OF ICT SECURITY

2.130 The Shared Services ICT governance statement mandates a whole-of-government meeting of chief information officers.[21] The meeting was a forum for discussion and consideration of strategic whole-of-government ICT issues and supported the Shared Services Governing Committee.

2.131 The Shared Services Governing Committee (see Figure 1) assumed the role of the whole-of-government meeting of chief information officers in providing a forum for information security discussions, and approval of information security policies and procedures. However, this changed, when this happened is uncertain, and the Shared Services' Security and Risk Management Committee was given the responsibility to oversee Shared Services ICT Security.

2.132 Audit notes from considering meeting minutes that the Shared Services Governing Committee maintained a watching brief on ICT projects, but did not consider emerging information security issues, such as access to social networking sites and mobile devices. No new information security draft policies were brought before it, although it did consider some amendments to policy and procedure. It did not consider the adoption of the Commonwealth's *Information Security Manual* as the foundation of ICT security policy in the ACT Government.

2.133 A Shared Services officer advised that the Information Strategy Committee, a sub-committee of the Strategic Board, would endorse future ICT security policy.

2.134 This arrangement is in its formative stages, given this it is important that Recommendation 1 be progressed.

[20] Available at the Territory Records Office website: http://www.territoryrecords.act.gov.au

[21] *ICT Services Governance Statement* Version 3, November 2009, page

CHIEF MINISTER AND CABINET DIRECTORATE

Government Information Office

2.135 The *Governing the City State: One ACT Government – One ACT Public Service* report (Hawke report) of February 2011 recommended the appointment of a Chief Information Officer within the Chief Minister and Cabinet Directorate.

2.136 In response to the report's recommendation, the ACT Government funded the Government Information Office from 2011-12.

2.137 The aims of the Government Information Office are to:

- develop and implement across-government high level strategic ICT priority settings;
- support senior governance arrangements to oversee the ICT Strategy; and
- enable improved prioritisation of the Government's investment in ICT.

2.138 The Government Information Office is to implement the ACT Government's *ICT Strategic Plan*. Under the plan, the ACT Government will:

- make living in Canberra easier by developing, with the community, an integrated, comprehensive and affordable range of readily accessible online services;
- improve return on investment on public expenditure on ICT through implementing and sharing higher quality, more resilient systems;
- use ICT to promote Open Government and online community engagement;
- contribute to the achievement of its environmental targets by improving the energy efficiency of its ICT infrastructure and promoting the use of ICT to assist other sustainability initiatives; and
- develop its workforce and partnerships to provide the future capacity and skills to implement its ICT programs and strategies.

2.139 The Government Information Office does not have a major role in information security, as do similarly named offices in other jurisdictions. However, given its broad strategic role, communication between this Office and other areas that are directly accountable for protective, information and ICT security, is important.

Cabinet documents

2.140 Cabinet documents are subject to the Protective Security Policies and Guideline's document classification requirements. Supplementing these are additional requirements found in the Cabinet Handbook, issued by the Chief Minister and Cabinet Directorate.

2.141 Electronic copies of cabinet documents are not stored in a records management system, but instead are kept on a dedicated network drive maintained by SSICT. SSICT have set up access to this drive in accordance with instructions from the Chief Minister and Cabinet Directorate.

APPENDIX A: AUDIT CRITERIA, APPROACH AND METHOD

AUDIT CRITERIA

- The whole-of-government environment for protective security-information security–ICT security is well defined and communicated.
- Whole-of-government ICT security policies and procedures are promoted to directorates.
- Whole-of-government ICT security policies, procedures and practices are monitored by senior management committees.
- Directorates are informed of their responsibilities for whole-of-government information security-ICT management.
- Shared Service directorate maintains a service level agreement that covers ICT with each directorate.
- Each ICT system is covered by a system security plan, or threat and risk assessment.
- Shared Services ICT on-site teams actively promote information security requirements in directorates where they are located.
- All information, electronic and paper based, can be protected through the appropriate security classification.
- Information classification systems conform to better practice, and those used by the Commonwealth.
- Directorates responsible for whole-of-government protective security-information security-ICT security are co-ordinated in their approach to the development, promotion and oversight of compliance with ICT security policy and procedure.

AUDIT APPROACH AND METHOD

The performance audit was conducted under the authority of the *Auditor-General Act 1996*, and in accordance with the principles, procedures, and guidance contained in Australian Auditing Standards relevant to performance auditing. These standards prescribe the minimum standards of professional audit work expected of performance auditors. Of particular relevance is the professional standard on assurance engagements - *ASAE 3500 Performance Engagements*.

The audit approach and methodology consisted of:

- reviewing literature and work undertaken on this subject by other jurisdictions;

- identifying those agencies who are responsible for whole-of-government policies and procedures and determining their administrative role and assessing the degree to which they fulfilled their functions; and
- briefings, interviews, correspondence and reporting with and to relevant agency staff.

APPENDIX B: SHARED SERVICES ICT POLICIES AND PROCEDURES

A Guide to Getting Started with a Website
Access Control Policy
Access to the ACT Government W: Drive Policy
ACT Government Domain Name Administration Policy
Additional requirements for Website Development
Australian Government Domain Name Policies
Business Case Guidelines and Template
Business Continuity Management Policy
Change Management Policy (ICT staff intranet)
Common (Whole-of-Government) Operating Environment Policy
Common (Whole-of-Government) Operating Environment Standard
Configuration Management
Critical Response and Incident Reporting Policy
Development of a Governance Structure for Projects with a Significant IT Component Guidelines
Encryption Policy
Encryption Standard
Freedom of Information On-line – Open Government Website Fact Sheet
Gateway Environment Policy
Guide to Mobile Device Usage
Guidelines for the preparation of a Content Management Strategy
ICT Security Policy
ICT Services Governance Statement
ICT Workstation Configuration Policy (ICT staff intranet)
Loss of Tokens for VPN Access Policy (ICT staff intranet)
Management of Privileged Accounts Policy
Management of Projects with an IT Component Policy
MARVAL Service Management System Policies (ICT staff intranet)
Metadata for Web-based Resources Policy
Metadata for Web-based Resources Standard
Mobile Devices Policy
Monitoring and Logging Standard
Online FOI Publication Policy
Password Policy
Password Standard

Policy Advice
Policy Advice
Policy Waiver Procedure
Publishing FOI material to the Open Government website
Release Management Policy
Remote Access to the ACT Government ICT Environment Policy
SafeGuard Laptop Encryption fact sheet
Security Policy Framework Guide
Security Policy Framework Guide
Server Build Policy (ICT staff intranet)
Server Build Standard (ICT staff intranet)
Servers for Small Sites Policy (ICT staff intranet)
Shared ICT Business Applications Policy
Statement of Responsibilities for ICT Services
Threat and Risk Assessment Process
Threat and Risk Assessment Report Templates
User IDs and Passwords
User IDs and Passwords Standard
Using Classified and/or Sensitive information in Non-production Environments
Virtual Separation of Servers Policy (ICT staff intranet)
Website Development and Management Standard
Website Policy
Whole-of-Government Acceptable Use of ICT Resources Policy
Workstation Administrator Password Management Policy (ICT staff intranet)

APPENDIX C: TERRITORY RECORDS OFFICE RECORDKEEPING STANDARDS, GUIDELINES AND RECORDS ADVICES

The Territory Records Office issues standards, guidelines and record advices.

Standards are notifiable instruments. Each has an accompanying guideline that is not a notifiable instrument.

Standard/Guideline 5: Recordkeeping and Outsourced Government Business)

Standard/Guideline 6: Digital Records

Standard/Guideline 8: Business Continuity and Records Management

Standard/Guideline 9: Records Digitisation and Conversion

Standards and guidelines are listed on the Territory Records Office website http://www.territoryrecords.act.gov.au/

The Territory Records Office also issues Records Advices. These are a brief introduction to records management topics.

Relevant advices are:

1. What is a record?

5. Electronically created records

7. Preparation for the implementation of an Electronic Records Management System (ERMS)

21. Security classification Cabinet documents

22. Security classification of non-Cabinet documents

28. Functional directories on shared drives

36. Destruction of ACT Government records

39. Vital records

50. Retention and storage of digital photographs and images

53. Managing web content as records

54. Use of portable electronic data storage devices

55. Web 2.0 - Social Networking and Collaboration Applications and Recordkeeping

65. Managing Security for Electronic Folders and Documents on Shared Drives

AUDIT REPORTS

Reports Published in 2011-12	
Report No. 2 / 2012	Whole-of-Government Information and ICT Security Management and Services
Report No. 1 / 2012	Monitoring and Minimising Harm Caused by Problem Gambling in the ACT
Report No. 06 / 2011	Management of Food Safety in the Australian Capital Territory
Report No. 05 / 2011	2010-11 Financial Audits
Report No. 04 / 2011	Annual Report 2010-11
Reports Published in 2010-11	
Report No. 03 / 2011	The North Weston Pond Project
Report No. 02 / 2011	Residential Land Supply and Development
Report No. 01 / 2011	Waiting Lists for Elective Surgery and Medical Treatment
Report No. 10 / 2010	2009-10 Financial Audits
Report No. 09 / 2010	Follow-up audit – Courts Administration
Report No. 08 / 2010	Delivery of Mental Health Services to Older Persons
Report No. 07 / 2010	Management of Feedback and Complaints
Report No. 06 / 2010	Annual Report 2009-10
Report No. 05 / 2010	Delivery of ACTION Bus Services
Reports Published in 2009-10	
Report No. 04 / 2010	Water Demand Management: Administration of Selected Initiatives
Report No. 03 / 2010	Delivery of Budget Initiatives
Report No. 02 / 2010	Student Support Services for Public High Schools
Report No. 01 / 2010	Performance Reporting
Report No. 08 / 2009	2008-09 Financial Audits
Report No. 07 / 2009	Annual Report 2008-09
Report No. 06 / 2009	Government Office Accommodation
Report No. 05 / 2009	Administration of employment issues for staff of Members of the ACT Legislative Assembly

Details of reports published prior to 2009-10 can be obtained from the ACT Auditor-General's Office or the ACT Auditor-General's homepage: http://www.audit.act.gov.au.

Details of reports published prior to 2002-2003 can be obtained from the ACT Auditor-General's Office or the ACT Auditor-General's homepage: http://www.audit.act.gov.au.

AVAILABILITY OF REPORTS

Copies of reports issued by the ACT Auditor-General's Office are available from:
ACT Auditor-General's Office
Level 4, 11 Moore Street
Canberra City ACT 2601

or

PO Box 275
CIVIC SQUARE ACT 2608

Phone (02) 62070833 / Fax (02) 62070826

Copies of reports are also available from the
ACT Auditor-General's Office Homepage: http://www.audit.act.gov.au