ACT AUDITOR–GENERAL'S REPORT

PHYSICAL SECURITY

REPORT NO. 6 / 2018

www.audit.act.gov.au

ISSN 2204-700X (Print)
ISSN 2204-7018 (Online)

ACT Audit Office

The roles and responsibilities of the Auditor-General are set out in the *Auditor-General Act 1996*.

The Auditor-General is an Officer of the ACT Legislative Assembly.

The ACT Audit Office undertakes audits on financial statements of Government agencies, and the Territory's consolidated financial statements.

The Office also conducts performance audits, to examine whether a Government agency is carrying out its activities effectively and efficiently and in compliance with relevant legislation.

The Office acts independently of the Government and reports the results of its audits directly to the ACT Legislative Assembly.

Accessibility Statement

The ACT Audit Office is committed to making its information accessible to as many people as possible. If you have difficulty reading a standard printed document, and would like to receive this publication in an alternative format, please telephone the Office on (02) 6207 0833.

If English is not your first language and you require the assistance of a Translating and Interpreting Service, please telephone Canberra Connect on 13 22 81.

If you are deaf or hearing impaired and require assistance, please telephone the National Relay Service on 13 36 77.

Audit Team

Brett Stanton
Hayley Tonkin
Callida Consulting (Paul Allen, Cherie Whitby, Fiona Emanuel & David Wimmer)
Meehan & Meehan Pty Ltd (Lloyd Meehan)

The support of Sophie Butler-Stratton and David Kelly is appreciated.

Produced for the ACT Audit Office by Publishing Services, Shared Services, Chief Minister, Treasury and Economic Development Directorate, ACT Government

Publication No. 18/0652

ACT Government Homepage address is: http://www.act.gov.au

ACT Audit Office

AUDITOR-GENERAL AN OFFICER OF THE ACT LEGISLATIVE ASSEMBLY

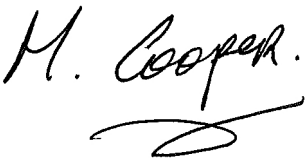
PA 17/12

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

Dear Madam Deputy Speaker

I am pleased to forward to you a Performance Audit Report titled 'Physical Security' for tabling in the Legislative Assembly pursuant to Subsection 17(5) of the *Auditor-General Act 1996*.

Yours sincerely



Dr Maxine Cooper
Auditor-General
31 May 2018

The ACT Audit Office acknowledges the Ngunnawal people as traditional custodians of the ACT and pays respect to the elders; past, present and future. The Office acknowledges and respects their continuing culture and the contribution they make to the life of this city and this region

Level 4, 11 Moore Street Canberra City ACT 2601 PO Box 275 Civic Square ACT 2608
T 02 6207 0833 **F** 02 6207 0826 **E** actauditorgeneral@act.gov.au **W** www.audit.act.gov.au

CONTENTS

SUMMARY

Physical security measures, be they procedural or actually physical, are designed to prevent or mitigate threats or attacks against people, information and physical assets. Each ACT Government directorate and agency is responsible for determining what physical security measures they need to implement as they are best equipped to determine their security risks and measures. Directorates and agencies are guided by the *ACT Government Protective Security Policy Framework* (the Framework) which is the responsibility of the Security and Emergency Management Branch in the Justice and Community Safety Directorate.

Overall conclusion

The *ACT Government Protective Security Policy Framework* is founded on the basis of a sound development process and initial issues in its implementation have been resolved. Physical security requirements in this framework are being effectively implemented by the audited directorates and agencies; Health Directorate, Education Directorate, Access Canberra, Venues Canberra and the Cultural Facilities Corporation. The effective implementation of the Framework reduces the risk of incidents occurring and, if there is an incident, increases the likelihood of it being appropriately managed. However, physical security is a matter that requires ongoing attention and routine assessment so that it is effectively managed.

The physical security needs of the Territory are likely to be better targeted if the Security and Emergency Management Committee of Cabinet is informed of operational priorities from a whole-of-government perspective on the highest risk areas overall and these are managed accordingly, rather than being determined on a directorate and agency basis.

Chapter conclusions

ACT GOVERNMENT PROTECTIVE SECURITY POLICY FRAMEWORK DEVELOPMENT, IMPLEMENTATION AND GOVERNANCE

While the development process for the *ACT Government Protective Security Policy Framework* was sound, there were issues with its implementation which took several years to resolve. Not all ACT Government directorates and agencies were included in the initial implementation of the Framework; notably for the purpose of this audit, the Cultural Facilities Corporation. This has been corrected.

While overall governance arrangements are appropriate there is a need to examine how the limited resources in some directorates and agencies can be supported with the skills and expertise that are dispersed in other directorates and agencies. An across ACT Government assessment needs to be

undertaken to determine how operational protective security advice, training and dissemination of better practice can best be provided.

AGENCIES' PHYSICAL SECURITY RISK MANAGEMENT

The Health Directorate, Education Directorate, Access Canberra, Venues Canberra and the Cultural Facilities Corporation have assessed physical security risks as required by the *ACT Government Protective Security Policy Framework*. The Health Directorate, while undertaking a rolling series of site risk assessments, needs to keep this program up-to-date as there are some sites that have not been assessed for over five years. The Education Directorate and Access Canberra need to undertake site-specific risk assessments.

AGENCIES' MANAGEMENT OF PHYSICAL SECURITY

Governance arrangements regarding protective security roles and responsibilities and current policies and procedures for the Health Directorate, Education Directorate, Access Canberra, Venues Canberra and Cultural Facilities Corporation were found to be effective in supporting the implementation of operational activities to meet the requirements of the *ACT Government Protective Security Policy Framework*.

These directorates and agencies had established processes to promote an effective security risk culture, including raising awareness of security issues through the implementation of training and other information and communication measures. Site-specific operational improvements were recommended to directorates and agencies where required. These are not reported in this audit for security reasons.

Key findings

ACT GOVERNMENT PROTECTIVE SECURITY POLICY FRAMEWORK DEVELOPMENT, IMPLEMENTATION AND GOVERNANCE	Paragraph
The process for developing the *ACT Government Protection Security Policy Framework* and *ACT Government Physical Security Principles* involved consultation with members of the former ACT Security-in-Government Committee, the former Security and Emergency Planning Group and the Security and Emergency Management Senior Officials Group. It resulted in a policy framework aligned with national practice, but which is tailored to meet the needs of the Territory.	2.14
While governance is sound overall, an assessment needs to be undertaken to determine what operational support is required for directorates and agencies to identify and implement physical security arrangements and how best this can be provided. There is no specific ACT Government area whose role is to support directorates and agencies by providing operational protective security advice and training. The Shared Services ICT Protective Security Team has, on occasion, provided this advice to other directorates and agencies.	2.47

A *Protective Security Policy Framework Communications Strategy* and *Protective Security Communications, Engagement and Education Plan* was developed by the Justice and Community Safety Directorate to support the implementation of the *ACT Government Protective Security Policy Framework* in 2014. Of the communication activities and channels to be delivered as part of the four phases of the rollout, there was evidence to substantiate some activities being delivered as part of the first phase. There was no evidence to substantiate that other planned communication activities and channels had actually occurred, specifically information briefing sessions relating to later phases of the implementation. Notably for this audit there is no evidence that the Cultural Facilities Corporation was consulted in the development of the *ACT Government Protective Security Policy Framework* and there is no evidence that it was included in the presentations and training opportunities. 2.60

The *ACT Government Protective Security Policy Framework*, the *ACT Government Protective Security Operational Procedures Manual* and implementation documentation indicates that the *ACT Government Protective Security Policy Framework* is intended to apply to all ACT Government directorates and agencies. However, the varying applicability statements, terminology and definitions used throughout the documents are inconsistent. This needs addressing. 2.75

The lack of clarity in the *ACT Government Protective Security Policy Framework* regarding agency applicability and a failure to contact all ACT Government agencies presents a risk of an operational area not being aware of their responsibilities for developing adequate protective security measures. Confirmation is needed that all directorates and agencies are now aware. 2.76

The ACT Government Protective Security intranet site is accessible to all ACT Government staff and provides useful information on protective security matters relevant to ACT Government directorates and agencies. A deficiency of the intranet site is that it does not include any information relating to the activities of the Shared Services ICT Protective Security team. The inclusion of this information, including links to relevant Shared Services ICT security documentation and information, would improve the usefulness of the intranet site. 2.81

Annual compliance reporting for the *Protective Security Policy Framework* has been achieved through a *Protective Security Policy Framework Compliance and Capability Assessment*. Only ACT Government directorates have been required to undertake this reporting to date, with compliance reported at a whole-of-directorate level. Similarly, only directorates have been required to participate in twice-yearly reporting against the *Protective Security Maturity Assessment*. The absence of reporting from other ACT Government agencies means that other relevant and useful information is not available to the Security and Emergency Management Branch. Furthermore, reporting at a whole-of-directorate level does not facilitate a detailed insight into physical security compliance with the *ACT Government Protective Security Policy Framework* at an operational level; reporting needs to be finer grained, especially for those directorates and agencies with diverse and discrete operational business units. 2.99

In the absence of an updated whole-of-government risk assessment with a protective security focus, there remains a reliance on directorate and agency level risk management practices to identify and manage their protective security risks including physical security risks. This could lead to physical security measures being implemented by each agency that are not commensurate to risk at an ACT Government level as a whole. There is a need to identify a regular mechanism, such as the strategic security risk assessment, for identifying and assessing the protective security risks faced by the ACT Government as a whole, so that the ACT Government has information whereby it can give priority to areas of highest overall risk to the Territory.	2.103

AGENCIES' PHYSICAL SECURITY RISK MANAGEMENT

	Paragraph
Venues Canberra has a high level of maturity in the assessment of risk and the management of physical security due to the nature of its work and its environment. Due to the nature of its work Access Canberra needs to undertake formal security risk assessments at each site level to provide an overall view of its security risk profile. This needs to inform future work in the security space and provide assurance that any gaps in current procedures, infrastructure and protocols have been identified and are being addressed.	3.18
Venues Canberra and Access Canberra managers advised that staff are aware of their physical security risks and have physical security control elements to manage these risks but that there was limited opportunity within the directorate to leverage their combined skills and experience in physical security management to improve practices across the Directorate and ACT Government as a whole. In a smaller agency, these same staff may hold the position of Agency Security Adviser or Agency Security Officer and therefore have the opportunity to attend security and emergency management meetings, but in a large agency they have no official role.	3.19
Site-specific security risk assessments have been underway in the Health Directorate since December 2013. This program of work is essential in identifying any physical security weaknesses and to enable subsequent actions to be prioritised. This program of work could be strengthened with the development of a forward work plan. Some sites have not had an assessment for a significant period of time and some facilities have not had an initial assessment. These need to be undertaken.	3.22
Physical security risks are known and managed both at the Education Directorate and school level, although the supporting documentation is not robust in some instances. At present, there is not a coordinated approach between school-specific physical security risk management and Directorate-level physical security risk management. The forthcoming development of the Directorate-level *Threat and Security Risk Assessment and Security Plan* represents an opportunity to strengthen engagement and future work plans with the Infrastructure and Capital Works Branch and schools in relation to physical security.	3.32
Although the 2014 *ACT Government Protective Security Policy Framework* was not implemented by the Cultural Facilities Corporation in 2014 (the Cultural Facilities	3.36

Corporation advised it was not communicated with as part of the initial implementation) it engaged security consultancies to identify security risks in its key facilities. In 2017 the Cultural Facilities Corporation reviewed and updated its protective security documentation to formally recognise the *ACT Government Protective Security Policy Framework*.

The *Chief Minister, Treasury and Economic Development Directorate Physical Security Plan* identified the need to progressively review the physical security risks at each of the Directorate's sites and locations with a view to developing a security action plan for each site. Fourteen reviews have been completed since the program commenced in 2016. Common themes identified in the reviews include coverage and quality of CCTV systems and issues with ICT communications rooms. The completion of all the site reviews will enable security action plans to be developed and prioritised to address any weaknesses. 3.42

In order to comply with the specific requirements of major national and international sporting and entertainment events the physical security standards and procedures implemented by Venues Canberra exceed those observed at other ACT Government locations. 3.47

Having a site security risk assessment conducted at all Access Canberra customer-facing sites is a priority for Access Canberra. The outcomes from these site assessments are expected to inform a Service Centre-level risk assessment which would then initiate implementation of physical security control elements, as required, to address weaknesses and monitor their effectiveness over time. This would enable the development of a formal security plan or work plan at the Access Canberra Service Centre-level. While Access Canberra's protective security risks, including physical security, are being formally documented at the Division-level, they do not provide sufficient detail to identify weaknesses at the Customer Service Centres. As the customer facing part of the business, the Customer Service Centre physical security risks need to be identified, assessed and managed. 3.50

The Health Directorate has demonstrated that it has a sound understanding of its physical security risk profile, through formal and informal mechanisms, and that risks are being managed. However, current physical security risk management could be strengthened by updating the enterprise-wide risk assessment and *Health Directorate Agency Security Plan* and undertaking security risk assessments at all Health Directorate sites. 3.55

The Education Directorate does not currently have a Security Plan. A whole-of-directorate *Security Threat and Risk Assessment* is currently being developed and it is expected that a whole-of-directorate Security Plan will also be developed from this exercise. This is due for completion by June 2018. 3.56

In the Cultural Facilities Corporation security plans were developed to address recommendations from the 2014 Security Risk Assessments. The development of revised security plans are scheduled as stage two of the consultancy, building on the risk assessments to develop operational procedures for security and counter terrorism. 3.59

The Cultural Facilities Corporation has taken significant steps in the last 12 months to be compliant with the *ACT Government Protective Security Policy Framework* and address gaps in its physical security controls. The Cultural Facilities Corporation now has in place protective security policy and governance arrangements for the ongoing management and monitoring of protective security.	3.60

AGENCIES' MANAGEMENT OF PHYSICAL SECURITY	Paragraph
All directorates and agencies reviewed in this audit have assigned an Agency Security Executive, Agency Security Adviser and Agency Security Officer as required by the *ACT Government Protective Security Policy Framework*. Only directorate and agency-level Agency Security Advisers attend relevant ACT Government protective security and emergency management committee meetings. A notable exception is that the Director, Venues Canberra has recently joined the Security and Emergency Management Policy Group and holds an appropriate security clearance to enable attendance at future Security and Emergency Management Senior Officials Group meetings.	4.11
All directorates and agencies reviewed as part of this audit have appropriate governance processes in place for the oversight of agency security requirements. Both the Health Directorate and the Education Directorate have established senior management security committees with a focus on security and emergency management issues, noting that for the Cultural Facilities Corporation, the Security Executive Group has only recently been established. For the Chief Minister, Treasury and Economic Development Directorate, it is the Senior Executive Management Group that considers protective security issues.	4.24
All directorates and agencies have incident reporting procedures in place that include reporting work health and safety incidents and near misses in RiskMan. Furthermore, all directorates and agencies have identified processes to report periodically on incidents and enable them to analyse incident data for specific risks or recurring themes.	4.92

Recommendations

RECOMMENDATION 1	WHOLE-OF-GOVERNMENT PROTECTIVE SECURITY SUPPORT ASSESSMENT

The Security and Emergency Management Branch (Justice and Community Safety Directorate) should coordinate an assessment of the physical security operational support needs across the ACT Government and present findings and recommendations to the Security and Emergency Management Senior Officials Group.

RECOMMENDATION 2 PROTECTIVE SECURITY POLICY FRAMEWORK APPLICABILITY

The Security and Emergency Management Branch (Justice and Community Safety Directorate) should:

a) review definitions and terminology to provide consistency between the *ACT Government Protective Security Policy Framework* and the *ACT Government Protective Security Operational Procedures Manual*;

b) update Section 3 of the *ACT Government Protective Security Policy Framework* to specify entities for which it is mandatory to apply the policy, and those for whom it is recommended; and

c) contact all ACT Government agencies, statutory bodies and entities to make them aware of the requirements of the *ACT Government Protective Security Policy Framework*.

RECOMMENDATION 3 PROTECTIVE SECURITY WEBPAGE

The Security and Emergency Management Branch (Justice and Community Safety Directorate) should strengthen access to protective security information by reviewing and providing links to relevant Shared Services ICT Protective Security documentation on the ACT Government Protective Security intranet site.

RECOMMENDATION 4 COMPLIANCE REPORTING

The Security and Emergency Management Branch (Justice and Community Safety Directorate) should:

a) amend the *Protective Security Policy Framework Compliance and Capability Assessment* and Director-General sign-off to require ACT Government directorates and agencies to:

   i) identify the business units and/or entities included in the report; and

   ii) gather information from all business units and/or entities to enable the identification of business units and entities with issues or areas of non-compliance at an operational level; and

b) notify relevant statutory bodies of their obligation to complete the annual *ACT Government* Protective *Security Policy Framework* compliance reporting, if this is not incorporated in the Directorate level reporting.

RECOMMENDATION 5 ACT GOVERNMENT PROTECTIVE SECURITY RISK ASSESSMENT

The Security and Emergency Management Branch (Justice and Community Safety Directorate) should undertake a whole-of-government protective security risk assessment encompassing physical security so that whole-of-government priorities are directed to the areas of greatest overall risk to the Territory. The whole-of-government protective security risk assessment should be reviewed and updated at scheduled intervals.

RECOMMENDATION 6	EDUCATION DIRECTORATE – SECURITY RISK ASSESSMENT

The Education Directorate should, on completion of its *Threat and Security Risk Assessment and Security Plan*, increase awareness of physical security risk for school based staff and implement a long-term rolling program of site-specific security risk assessments.

RECOMMENDATION 7	ACCESS CANBERRA – SECURITY RISK ASSESSMENTS

The Access Canberra Customer Coordination Division should engage with the Chief Minister, Treasury and Economic Development Directorate Agency Security Advisers to prioritise security risk assessments.

RECOMMENDATION 8	HEALTH DIRECTORATE – RISK MANAGEMENT

The Health Directorate should update its enterprise-wide risk assessment and *Health Directorate Agency Security Plan* to reflect: the work conducted since 2014; and the updated *ACT Government Protective Security Policy Framework*, and continued progress should be made to perform site-specific security risk assessments.

Agency responses

In accordance with subsection 18(2) of the *Auditor-General Act 1996*, the Chief Minister, Treasury and Economic Development Directorate (that includes Access Canberra and Venues Canberra), the Cultural Facilities Corporation, the Education Directorate, the Health Directorate and the Justice and Community Safety Directorate were provided with:

- a draft proposed report for comment. All comments were considered and required changes were reflected in the final proposed report; and
- a final proposed report for further comment. As part of this process, Territory entities were offered the opportunity to provide a statement for inclusion in the final report in the Summary Chapter.

No agency provided comments for inclusion in this Summary Chapter.

1 INTRODUCTION

Physical security

1.1 The *ACT Government Protective Security Policy Framework* (the Framework) was first implemented in 2014 and was re-developed and re-issued in 2017. It was modelled on the *Australian Government Protective Security Policy Framework* (2014) and followed the earlier *ACT Protective Security Policy and Guidelines* (2007).

1.2 The Framework establishes the principles for ACT Government directorates/agencies' management of security risks. The foreword to the Framework states that it:

> … articulates the government's expectation for protective security as a business enabler that allows directorates, agencies and the Commonwealth to work together securely in an environment of trust and confidence.

1.3 In the Framework physical security is defined as:

> … a combination of physical and procedural measures designed to prevent or mitigate threats or attacks against people, information and physical assets.

1.4 The *ACT Government Protective Security Operational Procedures Manual*, which provides operational guidance to directorates and agencies in relation to their protective security risks, states that a physical security program should aim to:

> **Deter** – these are measures implemented that adversaries perceive as too difficult, or needing special tools and training to defeat, for example, fences and signage.
>
> **Detect** – these are measures implemented to determine if an unauthorised action is occurring or has occurred, for example, alarms and CCTV.
>
> **Delay** – these are measures implemented to:
>
> - impede an adversary during an attack; or
> - slow the progress of a detrimental event to allow a response before Directorate information or physical assets are compromised, for example, access controls such as mechanical keys or access cards.
>
> **Respond** – these are measures taken, once a Directorate is aware of an attack or event, to prevent, resist or mitigate the attack or event, for example, security guards and police.
>
> **Recover** – these are measures taken to restore operations to normal (as possible) following an incident, for example, tradespeople to rectify damage and secure the property.

1.5 A physical security program is more than protection against security threats. It should address all hazards an agency may face in the protection of people, information, functions and physical assets. Physical security measures complement personnel security, information handling, communications and computer security procedures.

1.6 There are four mandatory requirements for physical security in the *ACT Government Protective Security Policy Framework*. As part of the revision to the Framework in 2017, these requirements were refined and re-defined. Table 1-1 shows these requirements as originally articulated in 2014 and as revised in 2017.

Table 1-1 *ACT Government Protective Security Policy Framework* Physical Security Mandatory Requirements

Reference	2014 Description	2017 Description
PHYSEC 1	Directors-General must provide clear direction on physical security through the development and implementation of a Directorate physical security policy and plan.	Directors-General and Chief Executive Officers must provide clear direction on physical security through adopting whole of government guidelines or the development and implementation of internal policy and procedures. These policies and procedures must be appropriate to the directorate or agency level of security risks or business requirements.
PHYSEC 2	Directorates must ensure they fully integrate protective security early in the process of planning, selecting, designing and modifying their facilities.	Directorates and agencies must ensure they fully integrate protective physical security early in the process of planning, selecting, designing and modifying their facilities to fulfil their protective security responsibilities.
PHYSEC 3	Directorates must ensure that any proposed physical security measure or activity does not breach relevant employer occupational health and safety obligations.	Directorates and agencies must ensure that any proposed physical security measure or activity does not breach relevant employer workplace, health and safety obligations.
PHYSEC 4	Directorates must show a duty of care for the physical safety of those members of the public interacting directly with the ACT Government. Where a Directorate's function involves providing services, the Directorate must ensure that clients can transact with the ACT Government with confidence about their physical wellbeing.	Directorates and agencies must show a duty of care for the physical safety of those members of the public interacting directly with the ACT Government. Where a directorate or agency function involves providing services, the directorate or agency must ensure that clients can conduct business with the ACT Government with confidence about their physical wellbeing

Source: *ACT Government Protective Security Policy Framework* 2014

Previous Audit Office reviews

1.7 The ACT Auditor-General's Report No. 2 of 2012 *Whole-of-Government Information and Communication Technology Security Management and Services* assessed whether the administrative structures and processes for whole-of-government ICT policies and procedures were well defined, managed and communicated. In doing this relevant information security and protective security issues were also considered.

1.8 At the time of the audit, as part of the revision of the *ACT Protective Security Policy and Guidelines*, ACT Security-In-Government Committee discussions were focussed on identifying which of the mandatory protective security requirements in the *Australian Government Protective Security Policy Framework* would be applicable to the ACT Government.

1.9 The audit report states:

> 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.
>
> It is in the ACT Government's interests that directorates 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 directorates.

1.10 The audit report concluded that the protection of the ACT Government network was robust, but three recommendations were made to improve whole-of-government security management practices.

1.11 The ACT Government's response to the report (14 September 2012) noted that in addition to the work being undertaken to clarify the roles and responsibilities of the ACT Government IT Security Advisor, the ACT Security-In-Government Committee and Directorate Agency Security Advisors:

> Work is also underway to formalise the relationship between Security and Emergency Management Branch (SEMB) within Justice and Community Safety Directorate, and Treasury's Shared Services ICT (Shared Services ICT) branch.

Audit objective and scope

Audit objective

1.12 The objective of the audit was to provide an independent opinion to the Legislative Assembly on the effectiveness of selected directorates/agencies' implementation of the physical security requirements of the *ACT Government Protective Security Policy Framework*.

Audit scope

1.13 The scope of the audit included consideration of the implementation of the physical security requirements of the *ACT Government Protective Security Policy Framework* as follows:

- Security and Emergency Management Branch (Justice and Community Safety Directorate) activities in developing and disseminating protective security policy and guidance across ACT Government, including the provision of training and support to directorates and agencies and monitoring and reporting on the implementation of the *ACT Government Protective Security Policy Framework*;

- Shared Services ICT Security's activities, in particular the role of the ACT Government IT Security Advisor (ITSA), in developing and disseminating IT security policy and guidance across ACT Government as it relates to physical security, including the provision of training and support to directorates and monitoring and reporting on IT security;
- selected directorates and agencies' identification and assessment of physical security risks and how these are addressed in directorate or agency specific protective security policies and procedures; and
- reviewing the implementation of physical security mandatory requirements in the selected directorate and agencies to assess compliance.

1.14 The directorates/agencies selected for the purpose of the audit included:

- Health Directorate;
- Education Directorate;
- Access Canberra and Venues Canberra (Chief Minister, Treasury and Economic Development Directorate); and
- Cultural Facilities Corporation.

Audit criteria, approach and method

Audit criteria

1.15 To form a conclusion against the objective, the following three questions were used as criteria and examined:

- Was the development, implementation and governance of the physical security requirements of the *ACT Government Protective Security Policy Framework* and related policies sound? Are there adequate mechanisms in place to provide guidance, training and evaluation of directorates and agencies' ongoing implementation of these policies?
- Have directorates and agencies undertaken a risk assessment to identify their specific physical security risks and addressed these through the development (where required) of agency-specific policies and procedures and controls that align with the *ACT Government Protective Security Policy Framework*?
- Have directorates and agencies effectively implemented physical security policies, procedures and controls for the physical safety of employees and members of the public?

Audit approach and method

1.16 The audit adopted the Audit Office's Performance Audit Methods and Practices and related Policies, Practice Statements and Guidance Papers. These policies and practices have been designed to comply with the requirements of the *Auditor-General Act 1996* and relevant professional standards (including *ASAE 3500 – Performance Engagements*).

1.17 The audit examined the implementation of the physical security requirements of the *ACT Government Protective Security Policy Framework* including:

- reviewing and analysing ACT Government and agency specific documentation and other evidentiary material relating to physical security to assess whether:
  - the development and dissemination of the physical security requirements of the *ACT Government Protective Security Policy Framework* and related policies was sound;
  - mechanisms are in place to provide adequate guidance and training;
  - directorates and agencies' implementation of these policies has been evaluated;
  - directorates and agencies have undertaken a specific physical security risk assessment and have developed policies, procedures and controls to mitigate or minimise identified risks;
  - directorates and agencies have effectively implemented physical security requirements at the sample locations and if the implementation is compliant with the *ACT Government Protective Security Policy Framework* mandatory requirements; and
  - directorates and agencies have effectively implemented physical security policies, procedures and controls to ensure the physical safety of employees and members of the public.
- holding discussions with staff from the selected directorates and agencies with responsibilities for physical security including governance, implementation, compliance and evaluation; and
- analysing a selection of auditee site locations against physical security requirements to determine the level of compliance with *ACT Government Protective Security Policy Framework* (2014) mandatory requirements. Details of sites assessed have been removed at the request of auditees.

1.18 In examining directorates and agencies' implementation of the physical security requirements of the *ACT Government Protective Security Policy Framework*, the audit considered the governance requirements of the *ACT Government Protective Security Policy Framework* and their implementation, and IT security requirements for security systems and IT infrastructure, in so far as they relate to physical security.

1.19 The *ACT Government Protective Security Policy Framework* was reviewed and updated in July 2017, however, due to the timing of the audit, directorates and agencies were reviewed against the 2014 version. The physical security mandatory conditions have not changed materially between the two versions.

1.20 Audit fieldwork was undertaken by Callida Consulting Pty Ltd on behalf of the ACT Audit Office. A subject matter expert, Mr Lloyd Meehan, from Meehan & Meehan Pty Ltd, was engaged by the ACT Audit Office to determine if ACT Government entities have effectively implemented physical security policies, procedures and controls to ensure the physical safety of employees and members of the public for the site locations selected.

1.21 Due to the sensitive nature of the information examined, only that of a broad nature is included in this audit report. Therefore information contained in the site assessments undertaken and documented by Meehan & Meehan Pty Ltd are not included in this report in order to protect the security of ACT Government people, information and physical assets.

1.22 Concurrently with providing a copy of this report for tabling to the Speaker of the Legislative Assembly the relevant Directors-General and Chief Executive Officers were provided with the site assessments as well as each directorate/agency's relevant Minister.

2 *ACT GOVERNMENT PROTECTIVE SECURITY POLICY FRAMEWORK* DEVELOPMENT, IMPLEMENTATION AND GOVERNANCE

2.1 This chapter discusses the development, implementation and governance of the *ACT Government Protective Security Framework* and related policies. It also reviews whether there are adequate mechanisms in place to provide guidance, training and evaluation of directorates and agencies' ongoing implementation of these policies.

Summary

Conclusion

While the development process for the *ACT Government Protective Security Policy Framework* was sound, there were issues with its implementation which took several years to resolve. Not all ACT Government directorates and agencies were included in the initial implementation of the Framework; notably for the purpose of this audit, the Cultural Facilities Corporation. This has been corrected.

While overall governance arrangements are appropriate there is a need to examine how the limited resources in some directorates and agencies can be supported with the skills and expertise that are dispersed in other directorates and agencies. An across ACT Government assessment needs to be undertaken to determine how operational protective security advice, training and dissemination of better practice can best be provided.

Key Findings

	Paragraph
The process for developing the *ACT Government Protection Security Policy Framework* and *ACT Government Physical Security Principles* involved consultation with members of the former ACT Security-in-Government Committee, the former Security and Emergency Planning Group and the Security and Emergency Management Senior Officials Group. It resulted in a policy framework aligned with national practice, but which is tailored to meet the needs of the Territory.	2.14
While governance is sound overall, an assessment needs to be undertaken to determine what operational support is required for directorates and agencies to identify and implement physical security arrangements and how best this can be provided. There is no specific ACT Government area whose role is to support directorates and agencies by providing operational protective security advice and	2.47

training. The Shared Services ICT Protective Security Team has, on occasion, provided this advice to other directorates and agencies.

A *Protective Security Policy Framework Communications Strategy* and *Protective Security Communications, Engagement and Education Plan* was developed by the Justice and Community Safety Directorate to support the implementation of the *ACT Government Protective Security Policy Framework* in 2014. Of the communication activities and channels to be delivered as part of the four phases of the rollout, there was evidence to substantiate some activities being delivered as part of the first phase. There was no evidence to substantiate that other planned communication activities and channels had actually occurred, specifically information briefing sessions relating to later phases of the implementation. Notably for this audit there is no evidence that the Cultural Facilities Corporation was consulted in the development of the *ACT Government Protective Security Policy Framework* and there is no evidence that it was included in the presentations and training opportunities. 2.60

The *ACT Government Protective Security Policy Framework*, the *ACT Government Protective Security Operational Procedures Manual* and implementation documentation indicates that the *ACT Government Protective Security Policy Framework* is intended to apply to all ACT Government directorates and agencies. However, the varying applicability statements, terminology and definitions used throughout the documents are inconsistent. This needs addressing. 2.75

The lack of clarity in the *ACT Government Protective Security Policy Framework* regarding agency applicability and a failure to contact all ACT Government agencies presents a risk of an operational area not being aware of their responsibilities for developing adequate protective security measures. Confirmation is needed that all directorates and agencies are now aware. 2.76

The ACT Government Protective Security intranet site is accessible to all ACT Government staff and provides useful information on protective security matters relevant to ACT Government directorates and agencies. A deficiency of the intranet site is that it does not include any information relating to the activities of the Shared Services ICT Protective Security team. The inclusion of this information, including links to relevant Shared Services ICT security documentation and information, would improve the usefulness of the intranet site. 2.81

Annual compliance reporting for the *Protective Security Policy Framework* has been achieved through a *Protective Security Policy Framework Compliance and Capability Assessment*. Only ACT Government directorates have been required to undertake this reporting to date, with compliance reported at a whole-of-directorate level. Similarly, only directorates have been required to participate in twice-yearly reporting against the *Protective Security Maturity Assessment*. The absence of reporting from other ACT Government agencies means that other relevant and useful information is not available to the Security and Emergency Management Branch. Furthermore, reporting at a whole-of-directorate level does not facilitate a detailed insight into physical security compliance with the *ACT Government Protective Security Policy Framework* at an operational level; reporting needs to be finer grained, especially for those directorates and agencies with diverse and discrete operational business units. 2.99

In the absence of an updated whole-of-government risk assessment with a protective security focus, there remains a reliance on directorate and agency level risk management practices to identify and manage their protective security risks including physical security risks. This could lead to physical security measures being implemented by each agency that are not commensurate to risk at an ACT Government level as a whole. There is a need to identify a regular mechanism, such as the strategic security risk assessment, for identifying and assessing the protective security risks faced by the ACT Government as a whole, so that the ACT Government has information whereby it can give priority to areas of highest overall risk to the Territory. 2.103

Development of the *ACT Government Protective Security Policy Framework*

2.2 The *ACT Government Protective Security Policy Framework* (the Framework) was modelled on the *Australian Government Protective Security Policy Framework* and followed the earlier *ACT Protective Security Policy and Guidelines* (2007).

ACT Protective Security Policy and Guidelines (2007)

2.3 Prior to the release of the Framework in 2014 the ACT Government had implemented the *ACT Protective Security Policy and Guidelines* (the 2007 Guidelines). The foreword to the 2007 Guidelines by the then Attorney-General stated:

> The ACT Protective Security Policy and Guidelines (the Guidelines) is the central policy document that will assist us in creating a robust security culture within the ACT Public Service.

2.4 The introduction to the 2007 Guidelines stated:

> It will assist all ACT Government directorates, their staff, contractors and clients and is designed to provide a transitional framework to ensure that ACT Government directorates approach the protection and security of people, assets and information in a way that is consistent across government.

Australian Government Protective Security Policy Framework

2.5 In June 2010 the *Australian Government Protective Security Policy Framework* was first developed and implemented. According to the Australian Government Attorney-General's Department:

> The PSPF has been developed to assist Australian Government entities to protect their people, information and assets, at home and overseas.
>
> The PSPF provides policy, guidance and better practice advice for governance, personnel, physical and information security. The 36 mandatory requirements assist Agency Heads to identify their responsibilities to manage security risks to their people, information and assets.

Cross Jurisdictional Chief Information Officer Working Group

2.6 In 2010 the Cross Jurisdictional Chief Information Officer Working Group recommended to the Council of Australian Governments that all States and Territories adopt the *Australian Government Protective Security Policy Framework*. The ACT Government agreed and the requirements of the *Australian Government Protective Security Policy Framework* were considered and refined for the ACT context.

ACT Government Protective Security Policy Framework

2.7 The *ACT Government Protective Security Policy Framework* requires all ACT Government directorates and agencies to take appropriate measures to protect people, information and physical assets, at home and overseas.

2.8 The foreword to the *ACT Government Protective Security Policy Framework* states:

> This Framework, supported by the ACT Government Protective Security Operational Procedures Manual, is designed to help directorates and agencies:
>
> a. identify vulnerabilities and their levels of security risk;
>
> b. achieve the mandatory requirements for protective security expected by the government;
>
> c. develop an appropriate security culture and proportionate measures to securely meet their business goals; and
>
> d. meet the expectations for the secure conduct of government business.

2.9 When first implemented in 2014 the *ACT Government Protective Security Policy Framework* contained 23 mandatory requirements relating to the following protective security categories:

- Governance (GOVSEC) – 12 mandatory requirements;
- Personnel Security (PERSEC) – 3 mandatory requirements;
- Information Security (INFOSEC) – 4 mandatory requirements; and
- Physical Security (PHYSEC) – 4 mandatory requirements.

2.10 In 2017 the *ACT Government Protective Security Policy Framework* was reviewed and refined. As part of this review a new category of protective security was added (Cyber Security – CYBERSEC) and the total number of mandatory requirements was reduced to 20:

- Governance (GOVSEC) – 8 mandatory requirements;
- Personnel Security (PERSEC) – 3 mandatory requirements;
- Information Security (INFOSEC) – 4 mandatory requirements;
- Physical Security (PHYSEC) – 4 mandatory requirements; and
- Cyber Security (CYBERSEC) – 2 mandatory requirements.

ACT Government Protective Security Operational Procedures Manual

2.11 A companion document to the *ACT Government Protective Security Policy Framework* has been developed; the *ACT Government Protective Security Operational Procedures Manual* (the Manual). This document operationalises the *ACT Government Protective Security Policy Framework* and stipulates the protocols, standards and guidelines required of ACT Government directorates and agencies to meet the mandatory requirements. Similar to the Framework, the Manual was first released in 2014, and was also revised and updated in 2017.

ACT Government Physical Security Principles

2.12 In 2016 the Security and Emergency Management Branch developed an additional guidance document specifically in relation to Physical Security. The *ACT Government Physical Security Principles* were introduced to provide detailed guidance on standards and options for physical security planning to achieve consistency and conformity with national standards across ACT Government. These Principles align with the Physical Security and Personnel Security mandatory requirements of the *ACT Government Protective Security Policy Framework* and the *Work Health and Safety Act 2011*.

Physical Security requirements alignment with Australian Government Protective Security Policy Framework

2.13 In determining the mandatory physical security requirements for the ACT Government (refer to paragraph 1.6), the Security and Emergency Management Branch and the cross-directorate ACT Security-In-Government Committee examined the relevance of the seven mandatory physical security (PHYSEC) requirements of the *Australian Government Protective Security Policy Framework* to the ACT Government. Three of the *Australian Government Protective Security Policy Framework* mandatory conditions, known as PHYSEC 2, 6 and 7, were not directly incorporated in the *ACT Government Protective Security Policy Framework* as physical security mandatory conditions, but were incorporated through other means as follows:

- Australian Government PSPF PHYSEC2 - identifying, protecting and supporting employees under threat of violence and reporting such incidents was included in the ACT Government PSPF as a Personnel Security (PERSEC) mandatory requirement;
- Australian Government PSPF PHYSEC6 - security measures that minimise or removes the risk of information and ICT equipment being made inoperable or inaccessible was not included as a mandatory requirement in the ACT Government PSPF but has been reflected in the ICT Security Policy that sits under the ACT Government PSPF; and
- Australian Government PSPF PHYSEC7 - plans and procedures to move up to heightened security levels in case of emergency and increased threat. Elements of PHYSEC 7 have been incorporated into PHYSEC 1 and PHYSEC 4.

2.14 The process for developing the *ACT Government Protection Security Policy Framework* and *ACT Government Physical Security Principles* involved consultation with members of the former ACT Security-in-Government Committee, the former Security and Emergency Planning Group and the Security and Emergency Management Senior Officials Group. It resulted in a policy framework aligned with national practice, but which is tailored to meet the needs of the Territory.

Governance

Roles and responsibilities for physical security

2.15 A number of different business units and groups have responsibility for protective security, including physical security, in the ACT Government:

- Security and Emergency Management Branch (Justice and Community Safety Directorate);
- Shared Services ICT (Chief Minister, Treasury and Economic Development Directorate);
- directorates and agencies; and
- various committees and working groups.

Security and Emergency Management Branch

2.16 The Security and Emergency Management Branch (Justice and Community Safety Directorate) was responsible for the development and implementation of the *ACT Government Protective Security Policy Framework* and is responsible for providing ongoing support, monitoring and reporting on the implementation of the Framework.

2.17 The Security and Emergency Management Branch provides whole-of-government coordination on issues relating to security and emergency management across the ACT. This coordination role involves the Security and Emergency Management Branch working closely with all ACT Government directorates and agencies, ACT Policing/Australian Federal Police, and relevant interstate and federal agencies. The responsibilities of the Security and Emergency Management Branch are described on the Justice and Community Safety Directorate website as follows:

> The Security and Emergency Management Branch is responsible for:
>
> - Whole-of-government coordination of the ACT's counter-terrorism arrangements.
> - Creating a security culture across ACT Government through protective security policy and education
> - Whole-of-government coordination of critical infrastructure protection.
> - Extending and maintaining Closed Circuit Television (CCTV) systems to improve community safety while ensuring the individual rights of ACT citizens are respected.

- Coordinating strategic policy advice on emergency management.

2.18 These strategic policy responsibilities are also detailed in the *ACT Government Protective Security Operational Procedures Manual* (the Manual) as follows:

> The Justice and Community Safety Directorate Security and Emergency Management Branch (JACS SEMB), in consultation key directorates and agencies, is responsible for developing whole-of government policy on public sector protective security.

2.19 The Security and Emergency Management Branch does not have a role in applying or implementing protective security at an operational level, but provides advice and guidance to ACT Government directorates and agencies to do so. It is the responsibility of directorates and agencies to provide training or awareness sessions in protective security to their staff and ensure staff with protective security roles have appropriate qualifications and/or experience.

2.20 The Security and Emergency Management Branch is the conduit between relevant Commonwealth departments and agencies and the ACT Government in security matters, provides administrative support to Security and Emergency Management committees and coordinates *ACT Government Protective Security Policy Framework* compliance reporting. Although it coordinates compliance reporting on the Framework it does not audit compliance.

ACT Government directorates and agencies

2.21 ACT Government directorate/agency responsibilities are detailed in the ACT Government *Protective Security Operational Procedures Manual*. The Manual states:

> Each Director-General (or Chief Executive Officer) is responsible for the protective security of their respective directorates and directorates. Directors-General are responsible to their Minister, and CEO's to their governing Board, for creating and maintaining an operating environment that:
>
> - safeguards its people and clients from foreseeable risks;
> - limits the potential for compromise of the confidentiality, integrity and availability of its official information and assets;
> - protects official assets from loss or misuse;
> - facilitates the appropriate sharing of official information in order for Government to effectively do business; and
> - supports the continued delivery of essential business in the face of disruptions caused by all types of hazards.

2.22 The *ACT Government Protective Security Policy Framework* governance security mandatory condition GOVSEC2 requires ACT Government directorates and agencies to appoint an Agency Security Executive (ASE), Agency Security Advisor (ASA) and may appoint an Agency Security Officer (ASO). In addition, Shared Services ICT must appoint an Information Technology Security Advisor (IT Security Advisor) who is responsible for ICT advice across all of ACT Government. The roles, as described in the *ACT Government Protective Security Policy Framework*, are shown in Table 2-1.

Table 2-1 Protective security roles and responsibilities as per GOVSEC2

Role	Acronym	Description
Agency Security Executive	ASE	Responsible for protective security policy and oversight of protective security practices
Agency Security Advisor	ASA	Responsible for providing advice on security risk and helping managers implement security measures and plans
Agency Security Officer	ASO	Responsible for the day-to-day protective security functions within the directorate/agency
Information Technology Security Advisor	IT Security Advisor	Responsible for information communication technology (ICT) security advice

Source: *ACT Government Protective Security Policy Framework*

2.23 Governance security mandatory condition GOVSEC2 requires directorates and agencies to appoint an Agency Security Executive and Agency Security Advisor. GOVSEC2 also allows for the appointment of Agency Security Officer(s) by directorates and agencies. Each directorate and agency reviewed as part of the audit had appointed staff to fulfil these positions are shown in Table 2-2.

Table 2-2 Directorate and agency protective security roles and responsibilities

Directorate	Agency Security Executive	Agency Security Advisor	Agency Security Officer
Chief Minister, Treasury and Economic Development Directorate	Director, Corporate Management	Senior Manager, Governance	Shared Services ICT Physical and Personnel Security Manager (ASA Operations) Shared Services ICT Protective Security Team
ACT Health Directorate	Executive Director, Business Support Services	Senior Manager, Protective Services and Transport	Security Operations Manager
Education Directorate	Director, Governance and Community Liaison Branch	Assistant Manager, Internal Audit and Risk Management Section, Governance and Community Liaison Branch	Agency Security Officer, Internal Audit and Risk Management, Governance and Community Liaison Branch
Cultural Facilities Corporation	Chief Executive Officer	Chief Financial Officer	Front of House Manager, Canberra Museum and Gallery, Building Services Manager, Canberra Theatre Centre, and Manager, Property and Grounds, Historic Places

Source: ACT Audit Office, based on information from directorates and agencies

Security and Emergency Management Committees

2.24 The ACT Government *Protective Security Operational Procedures Manual* states:

> The Protective Security Governance Framework is made up of a hierarchy of committees that develop ACT Protective Security policy at all levels.

2.25 Whole-of-government committees include:

- Security and Emergency Management Committee of Cabinet;
- Security and Emergency Management Senior Officials Group; and
- Security and Emergency Management Policy Group.

Security and Emergency Management Committee of Cabinet

2.26 The Security and Emergency Management Committee of Cabinet provides strategic direction for the ACT Government's preparation for emergencies under an all-hazards planning framework. The Committee meets on an 'as required' basis with security briefings to be provided to Cabinet at least twice a year.

Security and Emergency Management Senior Officials Group

2.27 The Security and Emergency Management Senior Officials Group is responsible for ensuring cooperation and coordination of activities between ACT Government directorates and agencies with respect to Emergency Management and Protective Security Policy. Its membership includes:

- the Directors-General of all ACT Government directorates;
- the Under Treasurer;
- the Chief Police Officer, ACT Policing,
- the Commissioner, Emergency Services Agency
- Chief Officers of ACT Fire and Rescue, ACT Ambulance Service, ACT State Emergency Services and ACT Rural Fire Service;
- the Chief Health Officer;
- the Public Information Coordinator; and
- the Chair, Security and Emergency Management Policy Group.

2.28 The Security and Emergency Management Senior Officials Group is established by the *Emergencies Act 2004* and is the primary mechanism for ensuring cooperation and coordination of activities with respect to whole of government protective security policy.

Security and Emergency Management Policy Group

2.29 The Security and Emergency Management Policy Group reports to the Security and Emergency Management Senior Officials Group. The role of the Security and Emergency Management Policy Group is to develop, implement and review specific security and emergency management matters for consideration by the Security and Emergency Management Senior Officials Group, including relevant counter terrorism and emergency management plans and procedures.

2.30 Its membership includes relevant senior officers (or the Agency Security Executive or Advisor) from all directorates as well as ACT Policing, Emergency Services Agency, Public Information Coordination, ActewAGL and Icon Water.

2.31 The Terms of Reference for the Security and Emergency Management Policy Group and the Security and Emergency Management Senior Officials Group require the committees to meet at least three times a year.

2.32 All of the committees have responsibility for both protective security and emergency management. The role of the Security and Emergency Management Senior Officials Group in the coordination of activities relating to protective security is specified in its Terms of Reference. For the Security and Emergency Management Policy Group this is less explicit with protective security tied in with emergency management and not considered independently.

Pre February 2017 arrangements

2.33 Up to February 2017, the whole-of-government committee structure included the ACT Security-In-Government Committee, which focussed on protective security only. This committee met quarterly and its membership included directorates' Agency Security Advisers, the Executive Director, Security and Emergency Management Branch, the ICT Security Senior Manager (Shared Services ICT) and the Director of Territory Records. This committee was instrumental in the development of the *ACT Government Protective Security Policy Framework* and had a direct reporting line to the Security and Emergency Management Senior Officials Group.

2.34 The ACT Security-In-Government Committee's Terms of Reference (2012) stated:

> The role of the ACT Security-In-Government Committee is to:
>
> - enhance protective security across all ACT Government directorates; and
> - be responsible for undertaking research, planning and policy development on matters relating to protective security including appropriate physical, personnel and information security measures, plans, policies and procedures. This includes, but is not limited to the ACT Protective Security Policy Framework (PSPF).

ACT Security Adviser Working Group

2.35 Following the disbanding of the ACT Security-In-Government Committee an ACT Security Adviser Working Group is proposed. Its draft Terms of Reference state:

> The purpose of the Security Adviser Working Group is to facilitate the ongoing improvement of operational level protective security arrangements and activities across all directorates and agencies.

2.36 Participation in the ACT Security Adviser Working Group is open to all Agency Security Advisers and associated protective security roles within ACT Government. Membership of the group, while managed by the Security and Emergency Management Branch, will be flexible to enable attendance by staff at meetings where a topic of particular relevance to their role is discussed.

2.37 At the time of audit fieldwork, the ACT Security Adviser Working Group had not yet met. The first meeting was held on 16 May 2018. Expanding membership of this group to include all Agency Security Advisers and officers with a protective security role is expected to provide an opportunity for operational managers at site level, for example, managers at Access Canberra Customer Service Centres, Venues Canberra and Community Health Centres to participate in an inter-agency forum to discuss protective security issues. Discussions during site visits identified that these staff would welcome the opportunity to leverage each other's skills and experiences, share lessons learnt and build a whole-of-government network or Community of Practice.

Shared Services Information Communication Technology

2.38 Shared Services ICT includes:

- the whole-of-government IT Security Advisor, who is responsible for information security (INFOSEC) and ICT security advice across government; and
- the Shared Service ICT Protective Security Team, which is focussed on physical security (PHYSEC) and personnel security (PERSEC) for the Chief Minister, Treasury and Economic Development Directorate.

IT Security Advisor

2.39 The IT Security Advisor has responsibility for the management of security measures and strategic direction for the implementation of ICT security across all ACT Government entities. This includes the development of the *ACT Government IT Security Policy* and related guidance and ensuring mechanisms are in place to protect the ACT Government's ICT systems against unauthorised access.

2.40 The ACT Government *Protective Security Operational Procedures Manual* states:

> The ITSA is responsible for the management of security measures to provide strategic direction for the implementation of ICT security for the ACT Government by:
>
> - facilitating communications between security personnel, information and communications technology (ICT) personnel and business personnel to ensure alignment of business and security objectives;
> - provide notification and support with relevant stakeholders during major incidents to ensure a collective and holistic responses to the incident;
> - provide strategic level guidance for Directorate ICT security programs;
> - ensuring compliance with ACT policy, standards, regulations and legislation;
> - the ACT Government's ICT systems are protected against unauthorised access or compromise; and
> - information in electronic form is stored, processed and/or communicated in accordance with legislation, ACT and Australian Government policies, and the information security requirements detailed in the Framework.

2.41 According to the ACT Government *Protective Security Operational Procedures Manual* 'the Shared Services ICT Security Senior Manager fulfils the role of ITSA for all ACT Directorates and agencies'.

2.42 From a physical security perspective the ACT Government IT Security Advisor has a limited role, providing advice in relation to specifications required for secure communications rooms as part of new builds or upgrades, and providing assurance that these specifications have been met. Day-to-day operations are managed by the directorates and agencies; this includes restricting access to communications rooms and following information security protocols.

Shared Service ICT Protective Security Team

2.43 The Shared Services ICT Protective Security Team conducts its physical security and personnel security activities within Shared Services and the broader Chief Minister, Treasury and Economic Development Directorate. For example, the Shared Services ICT Protective Security Team (in the Chief Minister, Treasury and Economic Development Directorate Agency Security Officer role) conducts physical security audits for Chief Minister, Treasury and Economic Development Directorate properties, and has prepared papers on whole-of-government approaches to a single access card and the use of closed circuit television (CCTV).

2.44 Neither the IT Security Advisor nor Shared Services ICT Protective Security Team provides training, however they do provide support to ACT Government directorates and agencies when requested.

2.45 In addition, the Shared Services ICT Protective Security Team has, on occasion, provided operational advice to other directorates and agencies on protective security, and more specifically, physical security. The provision of such advice and assistance is not a formal role for the team, but it has begun to do so because its knowledge and expertise is acknowledged and is being leveraged by other directorates and agencies. For example, the team has provided advice to the Health Directorate in relation to the physical security requirements for The Canberra Hospital Ward 11A Refurbishment. The formal recognition of such a role would provide a whole-of-government perspective and support for all ACT Government directorates and agencies in strengthening their security culture. However, before this is done an assessment of the need for such service is required.

2.46 The introduction of the ACT Security Adviser Working Group provides a forum for information sharing but this does not necessarily address the need for operational expertise support and training, as has been informally provided by Shared Services ICT Protective Security Team. An across-ACT Government assessment on operational support is needed. If there is a need, the merits of the Shared Services ICT Protective Security Team or another area formally having responsibility for whole-of-government operational advice and training and assisting with site risk assessments warrants consideration.

2.47 While governance is sound overall, an assessment needs to be undertaken to determine what operational support is required for directorates and agencies to identify and implement physical security arrangements and how best this can be provided. There is no specific ACT Government area whose role is to support directorates and agencies by providing operational protective security advice and training. The Shared Services ICT Protective Security Team has, on occasion, provided this advice to other directorates and agencies.

RECOMMENDATION 1	WHOLE-OF-GOVERNMENT PROTECTIVE SECURITY SUPPORT ASSESSMENT

The Security and Emergency Management Branch (Justice and Community Safety Directorate) should coordinate an assessment of the physical security operational support needs across the ACT Government and present findings and recommendations to the Security and Emergency Management Senior Officials Group.

Implementation of the *ACT Government Protective Security Policy Framework*

2.48 To assist in the implementation of the *ACT Government Protective Security Policy Framework* in 2014 the Security and Emergency Management Branch prepared:

- a *Protective Security Policy Framework Communication Strategy*; and
- an *ACT Government Protective Security Communications, Engagement and Education Plan 2014*.

Protective Security Policy Framework Communications Strategy

2.49 The *Protective Security Policy Framework Communications Strategy* was developed by the Security and Emergency Management Branch to:

> … develop and provide a training program to educate and engage directorate protective security staff, ensuring compliance with protective security mandates and that best practice protective security methodologies are followed.

2.50 The target audience for the communication of the *ACT Government Protective Security Policy Framework* was initially Agency Security Executives (ASE), Agency Security Advisers (ASA) and Agency Security Officers (ASO). The communication strategy identified that Agency Security Advisers and Agency Security Officers in particular had a role in promoting security awareness within their directorates and agencies and providing training for staff.

2.51 The *Protective Security Policy Framework Communications Strategy* developed by the Justice and Community Safety Directorate to support the implementation of the *ACT Government Protective Security Policy Framework* in 2014 identified the target audience as:

> [including] all ACT Government Directorates, authorities, agencies or other bodies established in relation to public purposes, including departments and authorities staffed under the ACT Public Sector Management Act (PSM Act), the *Financial Management and Accountability Act 1997.*

2.52 The *Protective Security Policy Framework Communications Strategy* identified that the *ACT Government Protective Security Policy Framework* was to be rolled out in four phases:

- Phase 1 Governance Security (GOVSEC) – July 2014;
- Phase 2 Personnel Security (PERSEC) – November 2014;

- Phase 3 Physical Security (PHYSEC) – February 2015; and
- Phase 4 Information Security (INFOSEC) – May 2015.

2.53 The *Protective Security Policy Framework Communications Strategy* included the following activities:

- information briefing sessions to internal and external stakeholders;
- an ACT Public Service Head of Service message for dissemination to all ACT Government employees;
- generic email notification to all Directors-General that could be disseminated to all staff;
- directorate Executive Briefings;
- notification email messages to be deployed to all members of Security and Emergency Management Senior Officials Group, former Security and Emergency Management Planning Group and former ACT Security-In-Government Committee (with emphasis on ACT Security-In-Government Committee members);
- a Protective Security e-Animation made available via whole-of-government media portal;
- security posters for work spaces and ICT screen savers;
- education programs for directorate specific security staff (Agency Security Executives, Advisers and Officers); and
- development of a whole-of-government Protective Security Discussion Forum, to allow for preliminary training and development of security personnel and development of whole-of-government protective security templates.

2.54 There was evidence that initial information briefing sessions for directorate-specific security staff (Agency Security Executives, Advisers and Officers) occurred during Phase 1 of the implementation. However, there was no evidence that other planned activities were undertaken for example:

- the ACT Public Service Head of Service message to all ACT Government employees (a draft message was prepared but there was no evidence that it was sent);
- generic email notification to all Directors-General;
- notification email messages to all members of Security and Emergency Management Senior Officials Group and ACT Security-In-Government Committee (with emphasis on ACT Security-In-Government Committee members); and
- ongoing education programs for directorate specific security staff (Agency Security Executives, Agency Security Advisers and Agency Security Officers).

2.55 Furthermore, the establishment of a whole-of-government Protective Security Discussion Forum, and in particular training and development of security personnel and development of whole-of-government protective security templates did not occur.

ACT Government Protective Security Communications, Engagement and Education Plan 2014

2.56 In addition to the *Protective Security Policy Framework Communication Strategy*, an *ACT Government Protective Security Communications, Engagement and Education Plan 2014* was developed to support the implementation of the *ACT Government Protective Security Policy Framework* and the *Protective Security Operational Procedures Manual*.

2.57 The objectives of the *Protective Security Communications, Engagement and Education Plan* were to:

- effectively implement the *ACT Government Protective Security Policy Framework* (PSPF) through training;
- provide support to senior management with strategic direction to reflect the *ACT Government Protective Security Policy Framework* through open discussions; and
- ensure Directors-General, Agency Security Executives and Agency Security Advisers are aware of their responsibilities for security through the implementation of this framework.

2.58 The *Protective Security Communications, Engagement and Education Plan* identified that effective implementation required linkages between risk identification and Agency Security Plans as well as training, including Agency Security Executive briefings and Agency Security Adviser and Agency Security Officer training. Evidence of an Agency Security Executive level PowerPoint presentation and Outlook training appointments and associated attachments indicates that some training was provided as part of the implementation of the *ACT Government Protective Security Policy Framework*.

2.59 The Security and Emergency Management Senior Officials Group and ACT Security-In-Government Committee reiterated to its membership the requirement for directorates/agencies to be involved in the provision of feedback during the development of the *ACT Government Protective Security Policy Framework* and ensure Agency Security Executives were aware of their roles and responsibilities. However, not all ACT Government entities, notably for this audit the Cultural Facilities Corporation, were members of these committees. There is no evidence that the Cultural Facilities Corporation was consulted in the development of the *ACT Government Protective Security Policy Framework* and there is no evidence that it was included in the presentations and training opportunities. The Cultural Facilities Corporation advised that it had not been consulted or included in training. This had implications for the Cultural Facilities Corporation's recognition and implementation of the *ACT Government Protective Security Policy Framework* (refer to paragraphs 2.72 to 2.73).

2.60 A *Protective Security Policy Framework Communications Strategy* and *Protective Security Communications, Engagement and Education Plan* was developed by the Justice and Community Safety Directorate to support the implementation of the *ACT Government Protective Security Policy Framework* in 2014. Of the communication activities and channels to be delivered as part of the four phases of the rollout, there was evidence to substantiate some activities being delivered as part of the first phase. There was no evidence to substantiate that other planned communication activities and channels had actually occurred, specifically information briefing sessions relating to later phases of the implementation. Notably for this audit there is no evidence that the Cultural Facilities Corporation was consulted in the development of the *ACT Government Protective Security Policy Framework* and there is no evidence that it was included in the presentations and training opportunities.

Applicability of the *ACT Government Protective Security Policy Framework*

Inconsistencies in wording of the applicability of the ACT Government Protective Security Policy Framework

2.61 A review of protective security documentation identified an inconsistent approach to the definition, applicability and implementation of the *ACT Government Protective Security Policy Framework* across ACT Government directorates and agencies.

2.62 The *ACT Government Protective Security Policy Framework*, as originally drafted in 2014 stated:

> As a policy of the ACT Government, Directorates must apply the ACT Government PSPF. It is a requirement for all non-government organisations that access national security classified information to adhere to the PSPF.

2.63 Throughout the rest of the document, the term 'directorate' was used when describing roles, responsibilities and actions to be undertaken. Mandatory conditions identified in the Framework were also phrased in terms of 'directorates', for example GOVSEC 1 stated:

> Directorates must provide all staff, including contractors, with sufficient information and security awareness training to ensure they are aware of, and meet the requirements of the Framework.

2.64 It is noted, however, that the foreword to the *ACT Government Protective Security Policy Framework*, as originally drafted in 2014, included a footnote which stated:

> For the purpose of this document the term Directorates refers to all directorates and statutory authorities within the ACT Government.

2.65 The *ACT Government Protective Security Operational Procedures Manual*, as originally drafted in 2014, similarly refers to 'directorates' when describing roles, responsibilities and actions to be undertaken, but also included a footnote in the foreword to the document which states:

> For the purpose of this document the term Directorates refers to all directorates and statutory authorities within the ACT Government.

2.66 Annexure 1 to the *ACT Government Protective Security Operational Procedures Manual*, as originally drafted in 2014, includes a glossary of terms and definitions. 'Directorate' is defined as follows:

> Includes all ACT Government Directorates, authorities, agencies or other bodies established in relation to public purposes, including departments and authorities staff under the ACT Public Sector Management Act (PSM Act), the *Financial Management and Accountability Act 1997*.

2017 amendments

2.67 While sections of the 2017 *ACT Government Protective Security Policy Framework* (including the mandatory requirements themselves) refer to directorates and agencies, the applicability statement at Section 3 of the 2017 version of the *ACT Government Protective Security Policy Framework* continues to refer to Directorates only. The footnote definition included in the 2014 version has also been removed.

2.68 The *ACT Government Protective Security Policy Framework*, as amended in 2017, now refers to 'directorates' in some parts and 'directorates and agencies' in other parts. With respect to the applicability of the *ACT Government Protective Security Policy Framework*, for example, Section 3 of the document states:

> As a policy of the ACT Government, Directorates must apply the ACT Government PSPF.

2.69 However, in other parts of the document including, for example, the mandatory conditions, the term 'directorates and agencies' is used. The *ACT Government Protective Security Operational Procedures Manual* (2017) states:

> All Directorates, agencies and portfolio agencies must apply the Protective Security Policy Framework (PSPF) to the extent their enabling legislation allows. This application is outlined in the *Public Sector Management Act 1994* (PSM Act).

Implementation of the Framework in 2014

2.70 When the *ACT Government Protective Security Policy Framework* was endorsed by Cabinet in 2014, the covering brief noted that statutory bodies (including the ACT Audit Office and ACT Electoral Office) were consulted. As direct engagement by the Security and Emergency Management Branch in the Justice and Community Safety Directorate was targeted at ACT Government directorates and other high risk directorates and agencies such as the Office of the Legislative Assembly, it is apparent that engagement with all ACT Government agencies did not occur.

2.71 While all directorates and some statutory bodies were members of the former ACT Security in Government Committee, former Security and Emergency Management Planning Group, and/or the Security and Emergency Management Senior Officials Group, membership of these groups did not extend to all ACT Government agencies and entities. As such, some statutory bodies would not have been engaged in the development of the *ACT Government Protective Security Policy Framework* nor had access to the ACT Security-In-Government Committee training, presentations and discussions, as part of the implementation phase.

Cultural Facilities Corporation

2.72 When the *ACT Government Protective Security Policy Framework* was implemented in 2014 the Cultural Facilities Corporation did not apply the Framework. The Cultural Facilities Corporation advised:

- it was not included in the consultation for, and development of, the 2014 *ACT Government Protective Security Policy Framework*, or the subsequent presentations and follow up action to check on its implementation; and
- it first became aware of the Framework as a result of attending protective security training organised through the Chief Minister, Treasury and Economic Development Directorate in December 2016. It sought further information in January 2017 but understood that the Framework only applied to ACT Government directorates.

2.73 Notwithstanding this, the Cultural Facilities Corporation advised that it decided to adopt the principles of the *ACT Government Protective Security Policy Framework* as best practice and commenced developing the *Cultural Facilities Corporation Protective Security Policy and Governance* document.

2.74 These issues have been addressed and the *ACT Government Protective Security Policy Framework* has been implemented in the Cultural Facilities Corporation.

2.75 The *ACT Government Protective Security Policy Framework*, the *ACT Government Protective Security Operational Procedures Manual* and implementation documentation indicates that the *ACT Government Protective Security Policy Framework* is intended to apply to all ACT Government directorates and agencies. However, the varying applicability statements, terminology and definitions used throughout the documents are inconsistent. This needs addressing.

2.76 The lack of clarity in the *ACT Government Protective Security Policy Framework* regarding agency applicability and a failure to contact all ACT Government agencies presents a risk of an operational area not being aware of their responsibilities for developing adequate protective security measures. Confirmation is needed that all directorates and agencies are now aware.

RECOMMENDATION 2	PROTECTIVE SECURITY POLICY FRAMEWORK APPLICABILITY

The Security and Emergency Management Branch (Justice and Community Safety Directorate) should:

a) review definitions and terminology to provide consistency between the *ACT Government Protective Security Policy Framework* and the *ACT Government Protective Security Operational Procedures Manual*;

b) update Section 3 of the *ACT Government Protective Security Policy Framework* to specify entities for which it is mandatory to apply the policy, and those for whom it is recommended; and

c) contact all ACT Government agencies, statutory bodies and entities to make them aware of the requirements of the *ACT Government Protective Security Policy Framework*.

ACT Government Protective Security intranet site

2.77 The ACT Government Protective Security intranet site, which is accessible to all ACT Government staff, is managed by the Security and Emergency Management Branch. It provides links to documentation and agency contacts as well as incident report forms and newly developed security handbooks. The intranet site provides:

- links to relevant documents including policy and operational procedures, guidance with respect to directorate and agency reporting obligations, information security principles, physical security principles, vetting policy, critical infrastructure, overseas business travel protocols and foreign delegations protocols;
- links to directorate and agency contacts;
- links to the *Protective Security Executive Handbook*, the *ACT Contact Reporting Form* and *Security Incident Report Form*; and
- links to Commonwealth Government protective security documents.

Protective Security Executive Handbook

2.78 The *Protective Security Executive Handbook* has recently been published in hardcopy and provided to ACT Public Service executives. This handbook provides executives with a summary of the information from the *ACT Government Protective Security Policy Framework* and its supporting documentation in relation to protective security better practice. It is also available via the intranet site.

ACT Government Security Awareness Handbook

2.79 An *ACT Government Security Awareness Handbook* for all ACT Government staff is currently in development. The Handbook will expand on the *ACT Government Protective Security Policy Framework* by detailing how protective security applies to all staff. It is currently at concept level and is unapproved, but a placeholder is already in place on the intranet site.

2.80 Discussions with the IT Security Advisor noted that the inclusion of a link from this intranet webpage to relevant Shared Services ICT documentation, including ICT security and Personnel security documentation and information, would be a useful addition and provide a single source for ACT Government Protective Security guidance.

2.81 The ACT Government Protective Security intranet site is accessible to all ACT Government staff and provides useful information on protective security matters relevant to ACT Government directorates and agencies. A deficiency of the intranet site is that it does not include any information relating to the activities of the Shared Services ICT Protective Security team. The inclusion of this information, including links to relevant Shared Services ICT security documentation and information, would improve the usefulness of the intranet site.

RECOMMENDATION 3 PROTECTIVE SECURITY WEBPAGE

The Security and Emergency Management Branch (Justice and Community Safety Directorate) should strengthen access to protective security information by reviewing and providing links to relevant Shared Services ICT Protective Security documentation on the ACT Government Protective Security intranet site.

Monitoring and reporting

Compliance reporting

2.82 During the implementation of the *ACT Government Protective Security Policy Framework* in 2014 and 2015, directorates and agencies were not required to report to the Security and Emergency Management Branch on compliance with respect to the implementation of the requirements of the Framework. This was to provide directorates and agencies with time to implement the *ACT Government Protective Security Policy Framework*, including allowing time for the development or updating of specific protective security policies and procedures.

2.83 However, as per the Governance mandatory requirement (GOVSEC 7), from July 2016 directorates have been required to provide a compliance report to the Security and Emergency Management Senior Officials Group. The Governance mandatory requirement (GOVSEC 7), as originally drafted in 2014, stated:

> Directorates must:
>
> - undertake an annual security assessment against the mandatory requirements detailed within this Framework; and
> - report their compliance with the mandatory requirements to the security and emergency management Senior Officials Group.
>
> The report must:
>
> - contain a declaration of compliance by the Director-General; and
> - state any areas of non-compliance, including details on measures taken to lessen identified risks.

2.84 In 2017 this requirement was updated to clarify that both directorates and agencies are required to undertake this activity. Prior to this only directorates had been providing a compliance report to the Security and Emergency Management Senior Officials Group.

Protective Security Policy Framework Compliance and Capability Assessment Template

2.85 Since 2016 directorates have been required to complete an annual assessment using the *Protective Security Policy Framework Compliance and Capability Assessment Template* developed by the Security and Emergency Management Branch. These assessments have subsequently been provided to the Security and Emergency Management Branch, which has coordinated a summary for presentation to the Security and Emergency Management Senior Officials Group on the basis of information provided through these assessments.

2.86 As part of the self-assessment, directorates have been required to outline existing measures that the directorate has in place against each mandatory requirement. The directorate has also been required to assess each of the existing measures as Good, Adequate or Marginal against the following definitions:

- Good – requirement is supported by Directorate policy and procedure with high level of compliance by all staff
- Adequate – requirement managed by established business practice appropriate to business needs and good level of compliance by all staff
- Marginal – some elements of requirement addressed or inconsistent application of policy

2.87 Following this assessment, directorates have then been required to give each mandatory requirement an overall compliance/capability rating as indicated in Table 2-3 below. The lower the score the more mature the agency is against the *ACT Government Protective Security Policy Framework*. The template also includes the option to identify future actions to strengthen compliance. The cover letter is signed as a declaration by the relevant Director-General.

Table 2-3 *ACT Government Protective Security Policy Framework* Compliance / Capability Matrix

Status	Compliance / Capability Rating	Description
Full Compliance	1	Mandatory requirement fully addressed
Partial Compliance	2	Some conditions of the mandatory requirement have been addressed and implementation will continue until full compliance is achieved
Maximum Capability	3	All conditions of the mandatory requirement have been addressed to the limit of the directorate's resources or appropriate to its business needs
Reduced Capability	4	Some conditions of the mandatory requirement have been addressed but currently unable to achieve maximum capability due to resource or other limitations
No Capability	5	Directorate has attempted to address the Mandatory Requirements but has no capability or capacity to implement necessary controls
Non-Compliant	6	No progress with implementing necessary controls

Source: Annual Protective Security Declarations

2.88 Any areas of non-compliance are identified as part of the declaration and ratings reported against the 23 mandatory requirements in accordance with the ratings scale in Table 2-3.

2.89 There are weaknesses in the reporting process, including:

- only directorates have been required to report. As such, there has been no visibility of the level of compliance by other ACT Government agencies; and
- directorates have only provided a single whole-of-directorate rating for each of the mandatory requirements of the *ACT Government Protective Security Policy Framework*.

2.90 Where a directorate is large and diverse a single rating potentially obscures the important, finer detail that may be apparent across different business units. For example, a single rating was provided for the Chief Minister, Treasury and Economic Development Directorate which did not take into account the diverse range of business activities in the directorate including, for example, Venues Canberra and Access Canberra and the specific protective security challenges faced by these business units. This increases the risk of incorrect reporting and reduces the effectiveness of the compliance reporting as a mechanism for identifying whole-of-government risks.

2.91 It is also noted that there is no compliance testing or subsequent follow-up by the Security and Emergency Management Branch or another party to validate the Directorate's self-assessment. As such, reliance is placed on the Director-General assuring themselves that there is sufficient evidence to support the assessment.

Maturity Assessment Tool

2.92 The Security and Emergency Management Branch has developed a *Maturity Assessment Tool*, which seeks to:

> … provide Directorates with a quick guide for analysing appropriate level of security procedures and protocols, determining the maturity of security culture and implementation priorities in relation to PSPF mandatory requirements.

2.93 This is a self-assessment tool, or health check, which is undertaken by directorates twice yearly to determine their level of protective security maturity. The *Maturity Assessment Tool* enables directorates to monitor changes and improvement over time.

2.94 Within the *Maturity Assessment Tool* key principles of the *ACT Government Protective Security Policy Framework* are grouped into ten overarching indicators, with a rating scale and matrix to ensure consistency in assessment. Of the ten groups only one relates specifically to Physical Security. Others relate to governance, personnel and information. Table 2-4 shows the *Maturity Assessment Tool*, its indicators and indicative ratings.

Table 2-4 Maturity Assessment Tool Indicators

Indicators	Commentary associated with an Advanced Rating
Governance Framework	Governance framework adheres to the *ACT Government Protective Security Policy Framework* requirements.
Security Appointments	Security appointments as primary roles are in place; personnel are trained and experienced and undergo ongoing professional development.
Security Knowledge	Security awareness is continually improved through ongoing education and awareness activities.
Security Management & Planning	Programs are in place to regularly review security threats, vulnerabilities, and risks.
Business Continuity	Business continuity plans are exercised with all personnel, physical and ICT security systems tested.
Management of Contractors	Contractors are cleared, briefed, and educated on all security obligations; aftercare program is in place
Physical Security	Access to facilities is controlled, recorded, and audited with all physical spaces appropriately zoned and restricted where appropriate.
Designated Security Assessed Positions	DSAP list is well maintained annually and reported to JACS SEMB.
Protective Security Training	Staff are aware of protective security requirements and training is ongoing
Information Security	Information security policies are established and reviewed within directorate's schedules.

Source: *Maturity Assessment Tool* and *ACT Government Protective Security Policy Framework* 2014

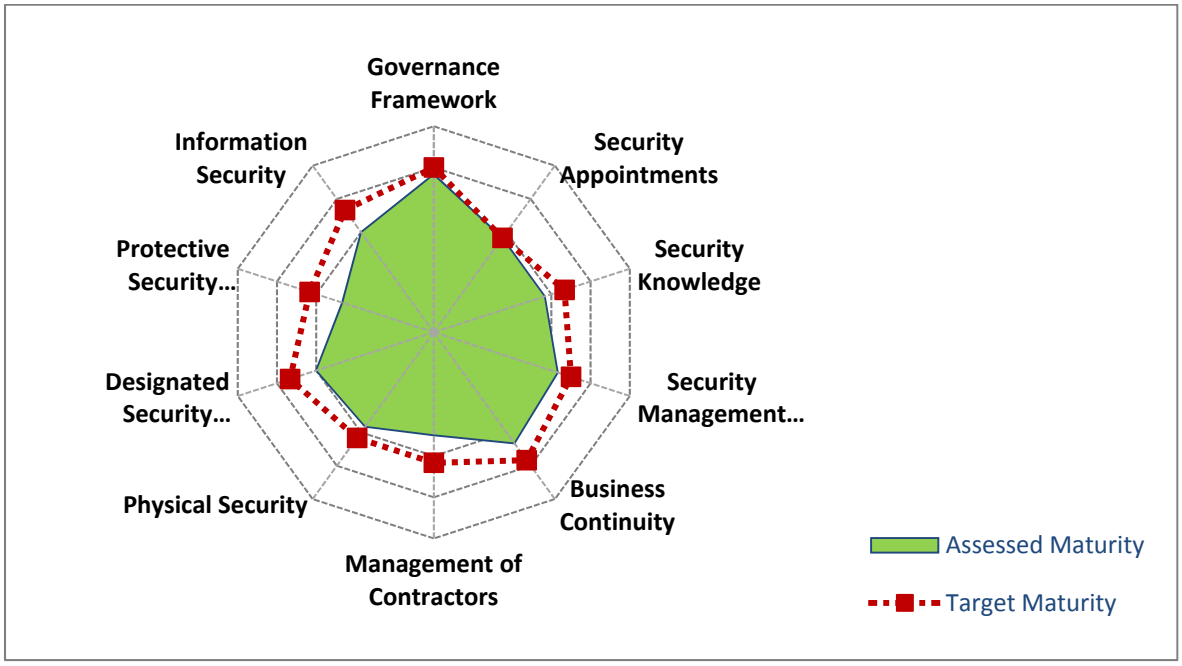
2.95 Directorates self-assess on a rating scale of 1 – Vulnerable, 2 – Basic, 3 – Intermediate and 4 – Advanced. The directorate determines its current rating, provides an agency rating goal and additional comments to put the rating in context. The individual scores are added to give an overall maturity score for the directorate.

2.96 A combined *Maturity Assessment Tool* assessment chart, which is provided to the Security and Emergency Management Policy Group and Security and Emergency Management Senior Officials Group, provides a whole-of-government graphical representation of its maturity against the *ACT Government Protective Security Policy Framework*. This includes a whole-of-ACT Government maturity rating against the indicators, a target rating and focus areas for the next 12 months. The focus areas and maturity targets are determined by the Security and Emergency Management Branch and are based on the directorates' responses to the Maturity Assessment Tool and knowledge of the protective security environment.

2.97 Similar to earlier comments on the *Protective Security Policy Framework Compliance and Capability Assessment Template* other ACT Government agencies have not been asked or required to participate in reporting against the Protective Security Maturity Assessment. This is a deficiency in the process.

2.98 A graphical representation of the Protective Security Maturity Assessment across ACT Government directorates as of April 2017 is shown in Figure 2-1.

Figure 2-1 Protective Security Maturity Assessment ACT Combined April 2017



Source: *Maturity Assessment Tool* and *ACT Government Protective Security Policy Framework* 2014

2.99 Annual compliance reporting for the *Protective Security Policy Framework* has been achieved through a *Protective Security Policy Framework Compliance and Capability Assessment*. Only ACT Government directorates have been required to undertake this reporting to date, with compliance reported at a whole-of-directorate level. Similarly, only directorates have been required to participate in twice-yearly reporting against the *Protective Security Maturity Assessment*. The absence of reporting from other ACT Government agencies means that other relevant and useful information is not available to the Security and Emergency Management Branch. Furthermore, reporting at a whole-of-directorate level does not facilitate a detailed insight into physical security compliance with the *ACT Government Protective Security Policy Framework* at an operational level; reporting needs to be finer grained, especially for those directorates and agencies with diverse and discrete operational business units.

RECOMMENDATION 4 COMPLIANCE REPORTING

The Security and Emergency Management Branch (Justice and Community Safety Directorate) should:

a) amend the *Protective Security Policy Framework Compliance and Capability Assessment* and Director-General sign-off to require ACT Government directorates and agencies to:

   i) identify the business units and/or entities included in the report; and

   ii) gather information from all business units and/or entities to enable the identification of business units and entities with issues or areas of non-compliance at an operational level; and

b) notify relevant statutory bodies of their obligation to complete the annual *ACT Government Protective Security Policy Framework* compliance reporting, if this is not incorporated in the Directorate level reporting.

Territory protective security risk assessments

Territory Wide Risk Assessment

2.100 The *Territory Wide Risk Assessment* is a strategic emergency risk management document that is a requirement of the *National Partnership Agreement – Natural Disaster Resilience.* The purpose of the *Territory Wide Risk Assessment* is to help inform directorates and agencies, emergency services and the community with making decisions on priorities for natural hazard emergency risk preparedness and mitigation. The initial assessment was developed in 2014 and was updated in November 2017. It is available on the ACT Emergency Services Agency website.

2.101 The *Territory Wide Risk Assessment* considered risks that impacted on people, property, the economy and the environment as well as on social and community services, and the level of emergency resources required for a significant and coordinated multi-agency response. The risks included epidemics, major infrastructure failure, biosecurity and hazardous waste as well as natural disasters such as floods, and bushfires. Protective security risks and controls, including physical security were not included in the *Territory Wide Risk Assessment*, noting its focus on natural hazards.

Strategic Security Risk Assessment

2.102 The Justice and Community Safety Directorate also advised that a whole-of-government strategic security risk assessment was undertaken in 2014-15, which was initiated as a result of the change in the national terrorism threat level in Australia. The strategic security risk assessment was used to inform the development of security policies in the ACT Government. The whole-of-government strategic security risk assessment has not been updated since 2014-15.

2.103 In the absence of an updated whole-of-government risk assessment with a protective security focus, there remains a reliance on directorate and agency level risk management practices to identify and manage their protective security risks including physical security risks. This could lead to physical security measures being implemented by each agency that are not commensurate to risk at an ACT Government level as a whole. There is a need to identify a regular mechanism, such as the strategic security risk assessment, for identifying and assessing the protective security risks faced by the ACT Government as a whole, so that the ACT Government has information whereby it can give priority to areas of highest overall risk to the Territory.

RECOMMENDATION 5	ACT GOVERNMENT PROTECTIVE SECURITY RISK ASSESSMENT

The Security and Emergency Management Branch (Justice and Community Safety Directorate) should undertake a whole-of-government protective security risk assessment encompassing physical security so that whole-of-government priorities are directed to the areas of greatest overall risk to the Territory. The whole-of-government protective security risk assessment should be reviewed and updated at scheduled intervals.

3 AGENCIES' PHYSICAL SECURITY RISK MANAGEMENT

3.1 This chapter examines the physical security risk management arrangements in place in audited directorates and agencies.

Summary

Conclusion

The Health Directorate, Education Directorate, Access Canberra, Venues Canberra and the Cultural Facilities Corporation have assessed physical security risks as required by the *ACT Government Protective Security Policy Framework*. The Health Directorate, while undertaking a rolling series of site risk assessments, needs to keep this program up-to-date as there are some sites that have not been assessed for over five years. The Education Directorate and Access Canberra need to undertake site-specific risk assessments.

Key findings

	Paragraph
Venues Canberra has a high level of maturity in the assessment of risk and the management of physical security due to the nature of its work and its environment. Due to the nature of its work Access Canberra needs to undertake formal security risk assessments at each site level to provide an overall view of its security risk profile. This needs to inform future work in the security space and provide assurance that any gaps in current procedures, infrastructure and protocols have been identified and are being addressed.	3.18
Venues Canberra and Access Canberra managers advised that staff are aware of their physical security risks and have physical security control elements to manage these risks but that there was limited opportunity within the directorate to leverage their combined skills and experience in physical security management to improve practices across the Directorate and ACT Government as a whole. In a smaller agency, these same staff may hold the position of Agency Security Adviser or Agency Security Officer and therefore have the opportunity to attend security and emergency management meetings, but in a large agency they have no official role.	3.19
Site-specific security risk assessments have been underway in the Health Directorate since December 2013. This program of work is essential in identifying any physical security weaknesses and to enable subsequent actions to be prioritised. This program of work could be strengthened with the development of a forward work	3.22

plan. Some sites have not had an assessment for a significant period of time and some facilities have not had an initial assessment. These need to be undertaken.

Physical security risks are known and managed both at the Education Directorate and school level, although the supporting documentation is not robust in some instances. At present, there is not a coordinated approach between school-specific physical security risk management and Directorate-level physical security risk management. The forthcoming development of the Directorate-level *Threat and Security Risk Assessment and Security Plan* represents an opportunity to strengthen engagement and future work plans with the Infrastructure and Capital Works Branch and schools in relation to physical security. 3.32

Although the 2014 *ACT Government Protective Security Policy Framework* was not implemented by the Cultural Facilities Corporation in 2014 (the Cultural Facilities Corporation advised it was not communicated with as part of the initial implementation) it engaged security consultancies to identify security risks in its key facilities. In 2017 the Cultural Facilities Corporation reviewed and updated its protective security documentation to formally recognise the *ACT Government Protective Security Policy Framework*. 3.36

The *Chief Minister, Treasury and Economic Development Directorate Physical Security Plan* identified the need to progressively review the physical security risks at each of the Directorate's sites and locations with a view to developing a security action plan for each site. Fourteen reviews have been completed since the program commenced in 2016. Common themes identified in the reviews include coverage and quality of CCTV systems and issues with ICT communications rooms. The completion of all the site reviews will enable security action plans to be developed and prioritised to address any weaknesses. 3.42

In order to comply with the specific requirements of major national and international sporting and entertainment events the physical security standards and procedures implemented by Venues Canberra exceed those observed at other ACT Government locations. 3.47

Having a site security risk assessment conducted at all Access Canberra customer-facing sites is a priority for Access Canberra. The outcomes from these site assessments are expected to inform a Service Centre-level risk assessment which would then initiate implementation of physical security control elements, as required, to address weaknesses and monitor their effectiveness over time. This would enable the development of a formal security plan or work plan at the Access Canberra Service Centre-level. While Access Canberra's protective security risks, including physical security, are being formally documented at the Division-level, they do not provide sufficient detail to identify weaknesses at the Customer Service Centres. As the customer facing part of the business, the Customer Service Centre physical security risks need to be identified, assessed and managed. 3.50

The Health Directorate has demonstrated that it has a sound understanding of its physical security risk profile, through formal and informal mechanisms, and that risks are being managed. However, current physical security risk management could 3.55

be strengthened by updating the enterprise-wide risk assessment and *Health Directorate Agency Security Plan* and undertaking security risk assessments at all Health Directorate sites.	
The Education Directorate does not currently have a Security Plan. A whole-of-directorate *Security Threat and Risk Assessment* is currently being developed and it is expected that a whole-of-directorate Security Plan will also be developed from this exercise. This is due for completion by June 2018.	3.56
In the Cultural Facilities Corporation security plans were developed to address recommendations from the 2014 Security Risk Assessments. The development of revised security plans are scheduled as stage two of the consultancy, building on the risk assessments to develop operational procedures for security and counter terrorism.	3.59
The Cultural Facilities Corporation has taken significant steps in the last 12 months to be compliant with the *ACT Government Protective Security Policy Framework* and address gaps in its physical security controls. The Cultural Facilities Corporation now has in place protective security policy and governance arrangements for the ongoing management and monitoring of protective security.	3.60

3.2 For each directorate and agency included in the audit, risk management processes in place were assessed for:

- compliance with the physical security requirements of the *ACT Government Protective Security Policy Framework*;
- identification and assessment of physical security risks; and
- development of policies and procedures to mitigate these risks.

3.3 To meet the requirements of the four physical security mandatory requirements (refer to paragraph 1.6) the directorate or agency was expected to have in place security risk management processes for the identification, assessment and ongoing monitoring and recording of agency risk. These risks should subsequently be addressed in the directorate or agency's security plan and physical security plan.

Chief Minister, Treasury and Economic Development Directorate

3.4 Two Chief Minister, Treasury and Economic Development Directorate business units were selected for inclusion in this audit; Venues Canberra and Access Canberra.

Venues Canberra

3.5 The Commercial Services and Infrastructure Division of the Chief Minister, Treasury and Economic Development Directorate provides corporate oversight of Venues Canberra. Venues Canberra manages GIO Stadium Canberra, Exhibition Park in Canberra (EPIC), the National Arboretum Canberra, Manuka Oval and Stromlo Forest Park. Some of Venues

Canberra's major clients include the ACT Brumbies, Canberra Raiders, Greater Western Sydney Giants, Cricket Australia, Summernats, National Folk Festival and the Handmade Markets. EPIC also manages a camping/caravan park on its site with over 200 spaces.

Access Canberra

3.6 Access Canberra is the business unit of the Chief Minister, Treasury and Economic Development Directorate responsible for managing the ACT Government's customer Service Centres, Contact Centre and online services to provide an integrated services hub. Through Access Canberra, ACT businesses, community groups and individuals can access information, support and undertake transactions with the ACT Government including vehicle registration and building development applications.

3.7 Access Canberra consists of five Divisions. Service Centres sit under the Customer Coordination Division with other customer facing business units including the Contact Centre and Complaints.

ACT Health Directorate

3.8 The Health Directorate has 57 facilities delivering a range of services in various locations around Canberra.

Education Directorate

3.9 The Education Directorate operates 87 public schools across 91 sites, and has Education Support Office staff in six locations across the ACT. Physical security in the 87 public schools is managed by each individual school with support from various business units within the Directorate including Internal Audit and Risk Management within the Governance and Community Liaison Branch, which has responsibility for implementation of the *ACT Government Protective Security Policy Framework* across the directorate, and the Infrastructure and Capital Works Branch, which facilitates large-scale maintenance and infrastructure projects for the Directorate as well as the coordination of physical security requirements for schools.

3.10 Non school-based Directorate staff are located in various offices across the ACT. The physical security arrangements for two office sites; the Hedley Beare Centre for Teaching and Learning (HBCTL) and Lyons Early Childhood School annex are managed by the Directorate. Physical Security arrangements at Education Directorate offices at Northbourne Avenue and Callum Offices are managed by the ACT Property Group.

Cultural Facilities Corporation

3.11 The Cultural Facilities Corporation is an ACT Government enterprise established under the *Cultural Facilities Corporate Act 1997*. The Cultural Facilities Corporation came into operation from 1 November 1997 to manage:

- the Canberra Theatre Centre;
- the Canberra Museum and Gallery (CMAG) including the Nolan Collection Gallery @ CMAG; and
- the ACT Historic Places including Lanyon Homestead, Calthorpes' House and Mugga-Mugga Cottage.

Risk management

3.12 The *ACT Government Protective Security Policy Framework* promotes a risk-based approach, where the implementation of the Framework in individual directorates and agencies should be driven and informed by the specific risks of the individual directorates and agencies.

Chief Minister, Treasury and Economic Development Directorate

3.13 In 2015 the Chief Minister, Treasury and Economic Development Directorate undertook a review of protective security risk across the directorate. The review was undertaken during the initial implementation phases of the *ACT Government Protective Security Policy Framework*, and as such, gaps against mandatory requirements were identified.

3.14 This review formed the basis for the *Enterprise Security Risk Assessment* for the Directorate and for developing the framework of documents to support compliance with the *ACT Government Protective Security Policy Framework*. Ten protective security landmark security work packages were identified to address the risks and enable conformance with the *ACT Government Protective Security Policy Framework*, which are shown in Table 3-1.

Table 3-1 Chief Minister, Treasury and Economic Development Directorate Security Treatment Program

	Landmark security work packages
1	Create and adequately provision the Agency Security Unit.
2	Map risk management processes and structures within the Directorate to avoid unnecessary duplication with the new security management role
3	Initiate whole-of-directorate security intelligence reporting/incident reporting.
4	Establish accurate appreciation of information holdings, including hardcopy, across the Directorate.
5	Review and audit POTs
6	Agree/coordinate with SEMB and SS-HR internal baseline/recruitment screening procedures and implement any changes by enhancing the recruitment pack and relevant internal processes.
7	Define and implement a security aftercare program
8	Rollout a security awareness training program
9	Define and implement physical security standards that will apply to all future construction and fit-out projects
10	Agree priorities for development and rollout of policies, protocols and procedures to enable conformance with the 12 GOVSEC, the 3 PERSEC, the 4 INFOSEC and the 4 PHYSEC 'mandatory conditions'.

Source: Chief Minister, Treasury and Economic Development Directorate Protective Security Risk Review (2015)

3.15 Implementation of the treatments has been monitored, in part, via directorate-level compliance and maturity assessment reporting to the Security and Emergency Management Senior Officials Group (refer to paragraphs 2.95 to 2.96). The Chief Minister, Treasury and Economic Development Directorate intends to engage a consultant to conduct a high level review of the Directorate's progress against the original risk review in 2018.

3.16 The *Chief Minister, Treasury and Economic Development Directorate Physical Security Plan* was signed off by the Agency Security Executive in March 2016. The Plan states that there will be a:

> Physical security review program [to] progressively review the physical security risk at each of the Chief Minister, Treasury and Economic Development Directorate locations/sites/buildings …

3.17 In relation to risk assessment at Venues Canberra and Access Canberra the report from the Audit Office's subject matter expert (Meehan & Meehan Pty Ltd) stated:

> Both Venues Canberra … and Access Canberra: have sound engagement with security risk, effective controls and well-developed doctrine.

3.18 Venues Canberra has a high level of maturity in the assessment of risk and the management of physical security due to the nature of its work and its environment. Due to the nature of its work Access Canberra needs to undertake formal security risk assessments at each site level to provide an overall view of its security risk profile. This needs to inform future work in the security space and provide assurance that any gaps in current procedures, infrastructure and protocols have been identified and are being addressed.

3.19 Venues Canberra and Access Canberra managers advised that staff are aware of their physical security risks and have physical security control elements to manage these risks but that there was limited opportunity within the directorate to leverage their combined skills and experience in physical security management to improve practices across the Directorate and ACT Government as a whole. In a smaller agency, these same staff may hold the position of Agency Security Adviser or Agency Security Officer and therefore have the opportunity to attend security and emergency management meetings, but in a large agency they have no official role.

Health Directorate

3.20 As the Health Directorate encompasses a range of services and is a very public facing Directorate, its physical security risk profile is a primary consideration in its day-to-day operations. The Directorate seeks to understand regular or constant risks and put in place a range of controls to mitigate these risks as much as possible.

3.21 The Health Directorate has undertaken a three to five year rolling program of site risk assessments. There is no set programming of sites for the rolling program, which is based instead on changing business priorities, the opening of new sites and new strategies that may come into effect (for example the National Crowded Places Strategy).

3.22 Site-specific security risk assessments have been underway in the Health Directorate since December 2013. This program of work is essential in identifying any physical security weaknesses and to enable subsequent actions to be prioritised. This program of work could be strengthened with the development of a forward work plan. Some sites have not had an assessment for a significant period of time and some facilities have not had an initial assessment. These need to be undertaken.

Education Directorate

Directorate-wide physical security risk assessments

3.23 The *Education Directorate - Strategic Risk Register 2017-18* identifies physical security risks and controls for the Directorate.

3.24 One strategic risk is identified in relation to physical security, which is rated as high after mitigating controls are taken into consideration, including emergency management and protective security policies, procedures and other activities. With staff and students across 91 school sites, office-based staff in six different office buildings and with the large numbers of staff, students and visitors accessing these premises each day, excursions off-site as well as a constantly changing security risk environment, this risk is likely to remain high.

Infrastructure and Capital Works Branch

3.25 The Infrastructure and Capital Works Branch is involved in the design of new buildings, as well as infrastructure upgrades. As such, it has a responsibility to ensure that physical security and work health and safety requirements are considered. Branch staff are trained in *Crime Prevention through Environmental Design* principles. The Infrastructure and Capital Works Branch conducts audits of school facilities using *Crime Prevention through Environmental Design* principles. The audits focus on the identification of key security issues and recommended areas for improvement, for example identifying sites that require additional security sensors.

3.26 Through its ongoing engagement with schools, the Branch has a good understanding of the physical security risks for individual schools, but this is not formally captured in physical security risk assessments, which are the responsibility of the Internal Audit and Risk Management Section within the Governance and Community Liaison Branch (refer to paragraph 3.27).

Site-specific assessments

3.27 A directorate-wide *Threat and Risk Assessment and Security Plan* is currently under development and it is expected that this will direct a future program of physical security-related work. Site–specific security risk assessments have been conducted by the Education Directorate's Agency Security Adviser (in the Internal Audit and Risk Management Section within the Governance and Community Liaison Branch) at schools identified as higher risk through RiskMan reporting or due to their location. To date seven site-specific risk assessments have been conducted. The Education Directorate has advised that another two are being planned.

3.28 Currently, security risks are identified and assessed through school-based *Emergency Management Plans* and risk registers, both of which include physical security aspects. Schools also complete an Education Directorate compliance checklist each semester, which is reported by the Principal to the School Board in June and November. It includes protective security with respect to: security of sensitive records, health safety and wellbeing, hazards identification, risk registers, accident/incident reporting, building maintenance plan and condition reporting, emergency management, evacuation and lockdown procedures and drills. The document references a range of ACT Government legislation, standards or policies but not the *ACT Government Protective Security Policy Framework*.

3.29 A review of the *Emergency Management Plans* provided by the Education Directorate, as well as those for the sites selected for audit, showed that templates are not being adequately modified to reflect the individual complexities of each school. In one example, a primary school with multiple pre-schools had not transferred this added complexity to other relevant components of its *Emergency Management Plan* such as the *Emergency Features of the School* and *Communication Methods* sections. Failure to comprehensively complete the template may result in a risk not being identified or appropriate planning put in place to mitigate or manage the risk. In this example, prior planning needs to be in place

and documented in the event of a security or emergency event at one campus, so that communication protocols are known.

3.30 In the Education Directorate it was recognised that executive staff and business managers in schools are not experts in risk and need support from the directorate's Agency Security Adviser and Agency Security Officer. There is a risk that schools may not have sufficient expertise in protective security and risk management to:

- identify those components of the template that are not relevant to their school;
- identify additional risks; or
- include the physical security control elements and site specific protocols to reflect their specific school environment.

Event and excursion-based risk assessments

3.31 A risk assessment for other sporting activities and excursions is incorporated into excursion paperwork. The standard risks for consideration include unacceptable student behaviour, student or staff illness or injury and transportation breakdown. Risk assessments are also required to be completed for school-based events, e.g. school fetes, and it is recognised that insurance is not issued for these events without a risk assessment. By identifying the risks and assessing the adequacy of the controls, including physical security controls, for school-based events and excursions the Education Directorate seeks to manage the physical security risks to students, staff and visitors.

3.32 Physical security risks are known and managed both at the Education Directorate and school level, although the supporting documentation is not robust in some instances. At present, there is not a coordinated approach between school-specific physical security risk management and Directorate-level physical security risk management. The forthcoming development of the Directorate-level *Threat and Security Risk Assessment and Security Plan* represents an opportunity to strengthen engagement and future work plans with the Infrastructure and Capital Works Branch and schools in relation to physical security.

RECOMMENDATION 6	**EDUCATION DIRECTORATE – SECURITY RISK ASSESSMENT**

The Education Directorate should, on completion of its *Threat and Security Risk Assessment and Security Plan*, increase awareness of physical security risk for school based staff and implement a long-term rolling program of site-specific security risk assessments.

Cultural Facilities Corporation

3.33 In 2014, the Cultural Facilities Corporation engaged security consultancies for its key facilities. As a result of these consultancies additional physical security control measures were implemented in the facilities. Since 2014, actions have been taken to strengthen the physical security control elements as recommended within the reports.

3.34 In 2017 the Cultural Facilities Corporation invested in meeting the requirements as set out in the *ACT Government Protective Security Policy Framework* including:

- using the *Protective Security Policy Framework Compliance and Capability Assessment* to identify areas of non-compliance with the *ACT Government Protective Security Policy Framework* in September 2017;
- developing a protective security policy, which was approved in September 2017;
- updating its Business Continuity Plan and Disaster Recovery Plan in 2017; and
- addressing *ACT Government Protective Security Policy Framework* risks in its *Strategic Risk Management Plan*.

3.35 Physical security is dealt with as a risk in the Strategic Risk Management Plan, which identifies actions to address this risk including:

- the preparation of the Cultural Facilities Corporation's *Protective Security Policy and Governance* policy document;
- working with the Justice and Community Safety Directorate to assist the Cultural Facilities Corporation to assess and rate specific Cultural Facilities Corporation security risks; and
- providing further security awareness and fraud awareness training.

3.36 Although the 2014 *ACT Government Protective Security Policy Framework* was not implemented by the Cultural Facilities Corporation in 2014 (the Cultural Facilities Corporation advised it was not communicated with as part of the initial implementation) it engaged security consultancies to identify security risks in its key facilities. In 2017 the Cultural Facilities Corporation reviewed and updated its protective security documentation to formally recognise the *ACT Government Protective Security Policy Framework*.

Security plans

3.37 The *ACT Government Protective Security Policy Framework* governance mandatory condition (GOVSEC 4) requires all directorates and agencies to prepare a security plan to manage security risks. The security plan must be updated or revised at least every two years.

Chief Minister, Treasury and Economic Development Directorate

3.38 The *Protective Security Policy and Governance* is the key security document for the Chief Minister, Treasury and Economic Development Directorate. This document provides the framework for a systematic and coordinated approach to security risk management and security in depth.

3.39 There is also a *Chief Minister, Treasury and Economic Development Directorate Physical Security Plan* as required under the physical security mandatory condition PHYSEC1. The *Chief Minister, Treasury and Economic Development Directorate Physical Security Plan* identified the need to progressively review the physical security risks at each of the Chief Minister, Treasury and Economic Development Directorate locations/sites/buildings.

3.40 The plan goes on to state that the reviews will be conducted by either the Shared Services ICT Protective Security team or consultants and the resultant reports would describe current physical security arrangements, identify risks and provide recommendations to correct any deficiencies identified. Once completed, a security action plan is intended to be developed to address the recommendations.

3.41 This program of reviews, consisting of eighteen sites, is currently being conducted by the Shared Services ICT Protective Security team. The physical security review checklist covers measures and controls such as: CCTV, security patrols, key security, physical barriers, lighting, alarms, access points, storage units, and ICT communications rooms. Risks are identified and recommendations (or suggested business improvements) have been proposed to address any weaknesses. Outcomes are reported to the Chief Minister, Treasury and Economic Development Directorate Senior Executive Management Group (EMG) as part of the six-monthly protective security report.

3.42 The *Chief Minister, Treasury and Economic Development Directorate Physical Security Plan* identified the need to progressively review the physical security risks at each of the Directorate's sites and locations with a view to developing a security action plan for each site. Fourteen reviews have been completed since the program commenced in 2016. Common themes identified in the reviews include coverage and quality of CCTV systems and issues with ICT communications rooms. The completion of all the site reviews will enable security action plans to be developed and prioritised to address any weaknesses.

Venues Canberra

3.43 Security Plans, encompassing physical security, are a core management document for each Venues Canberra site. The Security Plans use a consistent format and style, with tailoring to suit the types of events that occur at each location. The Security Plans undergo continuous review throughout the year, reflecting post-event learnings from operations.

3.44 Each Venues Canberra Security Plan identifies security procedures to be undertaken for major events, from perimeter controls through to bag inspections. Supporting documentation is embedded in each Security Plan including event run sheets, traffic management plans, emergency management plans, policies, briefs, checklists, and event schedule templates. In addition, there are site-specific procedures included in each Security Plan.

3.45 Venues Canberra seeks to ensure that each Security Plan remains active and capable of adapting to security risks that become apparent prior and during an event. This may involve relocating security guards, increased wanding (manual scanning) of attendees, or amending traffic control due to an accident. This enables Venues Canberra to vary the security landscape without requiring a new version of the Security Plan to be enacted.

3.46 Venues Canberra staff are also in close communication with the Security and Emergency Management Branch with respect to national and international experiences and threats. New or emerging risks are assessed using risk management software. Modifications to procedures, in ramping up or down of security measures based on an assessment of risk, occurs for all Venues Canberra events. Dependent on the event, and the hirer, on-site staff may need pre-accreditation checks, and the venue locked down in the days prior to the event. Access restrictions are in place for caterers, pre-match entertainers, and other service providers and all attendees need to be ticketed and undergo security checks at the gate.

3.47 In order to comply with the specific requirements of major national and international sporting and entertainment events the physical security standards and procedures implemented by Venues Canberra exceed those observed at other ACT Government locations.

Access Canberra

3.48 Physical security risk is formally documented at the Access Canberra Customer Coordination Division level in the *Access Canberra Customer Coordination Risk Plan 2017*. Physical security components are identified as risk sources, including aggressive customers, natural disasters, damage to infrastructure, and physical security of information.

3.49 There are no service centre or site-specific risk registers or security action plans. Each service centre delivers different services, has diverse building designs and locations, and services various clientele. As such, physical security may be managed differently and each centre will have its own physical security risks or issues that need to be specifically managed.

3.50 Having a site security risk assessment conducted at all Access Canberra customer-facing sites is a priority for Access Canberra. The outcomes from these site assessments are expected to inform a Service Centre-level risk assessment which would then initiate implementation of physical security control elements, as required, to address weaknesses and monitor their effectiveness over time. This would enable the development of a formal security plan or work plan at the Access Canberra Service Centre-level. While Access Canberra's protective security risks, including physical security, are being formally documented at the Division-level, they do not provide sufficient detail to identify weaknesses at the Customer Service Centres. As the customer facing part of the business, the Customer Service Centre physical security risks need to be identified, assessed and managed.

RECOMMENDATION 7 ACCESS CANBERRA – SECURITY RISK ASSESSMENTS

The Access Canberra Customer Coordination Division should engage with the Chief Minister, Treasury and Economic Development Directorate Agency Security Advisers to prioritise security risk assessments.

Health Directorate

3.51 The *Health Directorate Agency Security Plan* is based upon a process of identifying and assessing security compliance requirements and risks affecting the directorate, and identifying the protective security controls to protect against those risks. The Plan was developed in 2014 in accordance with the ACT Government requirements, the international standard for risk management (ISO 31000:2009) and Standards Australia's Handbook for security risk management (HB 167:2006).

3.52 The objectives of the *Health Directorate Agency Security Plan* are:

- the protection of ACT Health people, assets, information and operations;
- management and treatment of intolerable security risks identified within Enterprise Security Risk Assessments (ESRA); and
- provision of overarching guidance on security practice within the Health Directorate, to be applied in conjunction with supporting security documentation.

3.53 The security plan includes roles and responsibilities, identifies related documentation and has a section on physical security. It provides high level guidance only. Directorate policies and procedures and other guidance detail how the Directorate manages its physical control elements.

3.54 While there is a program of work to conduct site security assessments, these are pending. Progress to address this, will ensure that the ACT Health Directorate is aware of, and is able to actively monitor and manage site specific physical security risks across its facilities.

3.55 The Health Directorate has demonstrated that it has a sound understanding of its physical security risk profile, through formal and informal mechanisms, and that risks are being managed. However, current physical security risk management could be strengthened by updating the enterprise-wide risk assessment and *Health Directorate Agency Security Plan* and undertaking security risk assessments at all Health Directorate sites.

RECOMMENDATION 8 HEALTH DIRECTORATE – RISK MANAGEMENT

The Health Directorate should update its enterprise-wide risk assessment and *Health Directorate Agency Security Plan* to reflect: the work conducted since 2014; and the updated *ACT Government Protective Security Policy Framework*, and continued progress should be made to perform site-specific security risk assessments.

Education Directorate

3.56 The Education Directorate does not currently have a Security Plan. A whole-of-directorate *Security Threat and Risk Assessment* is currently being developed and it is expected that a whole-of-directorate Security Plan will also be developed from this exercise. This is due for completion by June 2018.

3.57 Under school-based management, schools are responsible in the main part for the physical security control elements in their school. While the ACT Education Directorate provides the policy frameworks and support from specialist teams, including funding for major physical security infrastructure, how physical security is managed at a school level is dependent on the experience and security awareness of the staff within each school.

Cultural Facilities Corporation

3.58 The Cultural Facilities Corporation *Protective Security Policy and Governance* document states:

> The Agency Security Executive Group will develop the Cultural Facilities Corporation Security Plan which will address significant Cultural Facilities Corporation-wide security risks. The Cultural Facilities Corporation security plan will be informed by the Cultural Facilities Corporation's security threat assessment and the annual Cultural Facilities Corporation risk assessment.

3.59 In the Cultural Facilities Corporation security plans were developed to address recommendations from the 2014 Security Risk Assessments. The development of revised security plans are scheduled as stage two of the consultancy, building on the risk assessments to develop operational procedures for security and counter terrorism.

3.60 The Cultural Facilities Corporation has taken significant steps in the last 12 months to be compliant with the *ACT Government Protective Security Policy Framework* and address gaps in its physical security controls. The Cultural Facilities Corporation now has in place protective security policy and governance arrangements for the ongoing management and monitoring of protective security.

4 AGENCIES' MANAGEMENT OF PHYSICAL SECURITY

4.1 This chapter discusses arrangements in place in the ACT Government directorates/agencies selected for the purpose of the audit, for the implementation of the physical security mandatory requirements of the *ACT Government Protective Security Policy Framework*.

Summary

Conclusion

Governance arrangements regarding protective security roles and responsibilities and current policies and procedures for the Health Directorate, Education Directorate, Access Canberra, Venues Canberra and Cultural Facilities Corporation were found to be effective in supporting the implementation of operational activities to meet the requirements of the *ACT Government Protective Security Policy Framework*.

These directorates and agencies had established processes to promote an effective security risk culture, including raising awareness of security issues through the implementation of training and other information and communication measures. Site-specific operational improvements were recommended to directorates and agencies where required. These are not reported in this audit for security reasons.

Key findings

	Paragraph
All directorates and agencies reviewed in this audit have assigned an Agency Security Executive, Agency Security Adviser and Agency Security Officer as required by the *ACT Government Protective Security Policy Framework*. Only directorate and agency-level Agency Security Advisers attend relevant ACT Government protective security and emergency management committee meetings. A notable exception is that the Director, Venues Canberra has recently joined the Security and Emergency Management Policy Group and holds an appropriate security clearance to enable attendance at future Security and Emergency Management Senior Officials Group meetings.	4.11
All directorates and agencies reviewed as part of this audit have appropriate governance processes in place for the oversight of agency security requirements. Both the Health Directorate and the Education Directorate have established senior management security committees with a focus on security and emergency management issues, noting that for the Cultural Facilities Corporation, the Security Executive Group has only recently been established. For the Chief Minister, Treasury	4.24

and Economic Development Directorate, it is the Senior Executive Management Group that considers protective security issues.

All directorates and agencies have incident reporting procedures in place that include reporting work health and safety incidents and near misses in RiskMan. Furthermore, all directorates and agencies have identified processes to report periodically on incidents and enable them to analyse incident data for specific risks or recurring themes. 4.92

Administrative arrangements

4.2 Administrative arrangements were considered in each ACT Government directorate or agency selected for the audit including the Health Directorate, Education Directorate; Access Canberra and Venues Canberra (Chief Minister, Treasury and Economic Development Directorate) and the Cultural Facilities Corporation. Administrative arrangements considered included:

- agency roles and responsibilities; and
- organisational oversight.

Roles and responsibilities

4.3 As discussed in Chapter 2 of this report Governance security mandatory condition GOVSEC2 requires directorates and agencies to appoint an Agency Security Executive, Agency Security Adviser and may appoint an Agency Security Officer. Each directorate or agency reviewed as part of this audit had appointed staff to fulfil these positions.

Chief Minister, Treasury and Economic Development Directorate

4.4 In the Chief Minister, Treasury and Economic Development Directorate agency security roles sit at the whole-of-directorate level rather than the operational level. While the Shared Services ICT Protective Security Team collectively takes on the role of the Agency Security Officer, it is not responsible for the day to day management of security at specific sites.

Venues Canberra and Access Canberra

4.5 There are no formal agency security roles within business units, including Access Canberra or Venues Canberra. However, supervisors at an operational level have responsibility for managing physical security as part of their day to day management responsibilities.

4.6 The Director, Venues Canberra has overall responsibility for the physical security for the Venues Canberra sites. The Director is supported by the Chief Operations Officer (COO) and day-to-day management is the responsibility of the venue managers.

4.7 Responsibility for the physical security of Access Canberra sites is managed by its building support services team. This team is responsible for building access cards and maintenance. Any potential physical security issues that require escalation will ultimately be referred to the Deputy Director, Projects, Governance and Support, who is responsible for support services.

Health Directorate

4.8 In addition to the security-specific roles identified in Chapter 2, the Health Directorate has an executive role of Director, Client Services, Security and Emergency. This executive is responsible for both protective security and emergency management in the directorate.

Education Directorate

4.9 In addition to the identified protective security roles identified in Chapter 2 the Infrastructure and Capital Works Branch has a role with respect to the physical security of schools and Education Directorate buildings. This includes responsibility for the external security fencing program and maintenance and upgrades to schools' security systems.

Cultural Facilities Corporation

4.10 In addition to the identified protective security roles identified in Chapter 2, the Cultural Facilities Corporation has established a Security Executive Group which includes the Business Unit Directors and the Chief Finance Officer. The Security Executive Group is responsible to the Chief Executive Officer for the ongoing development of the *Cultural Facilities Corporation Protective Security Policy and Governance* policy document and the oversight of protective security matters within the Cultural Facilities Corporation.

Summary

4.11 All directorates and agencies reviewed in this audit have assigned an Agency Security Executive, Agency Security Adviser and Agency Security Officer as required by the *ACT Government Protective Security Policy Framework*. Only directorate and agency-level Agency Security Advisers attend relevant ACT Government protective security and emergency management committee meetings. A notable exception is that the Director, Venues Canberra has recently joined the Security and Emergency Management Policy Group and holds an appropriate security clearance to enable attendance at future Security and Emergency Management Senior Officials Group meetings.

Organisational oversight

Chief Minister, Treasury and Economic Development Directorate

4.12 The Chief Minister, Treasury and Economic Development Directorate *Protective Security Policy and Governance* document outlines the directorate's governance and administrative arrangements for protective security.

4.13 The Chief Minister, Treasury and Economic Development Directorate *Protective Security Policy and Governance* document has identified the Chief Minister, Treasury and Economic Development Directorate Senior Executive Management Group as the forum to monitor and discuss issues relating to the implementation of the *ACT Government Protective Security Policy Framework* and protective security more broadly in the directorate. The Senior Executive Management Group consists of the Director-General, the Under Treasurer, the Executive Director Corporate and the Chief Finance Officer .

4.14 The Agency Security Adviser (Governance) reports to the Executive Management Group on a six monthly basis (June and December) on protective security and the *ACT Government Protective Security Policy Framework*; providing updates and also incident reporting for the preceding six months. If an issue arises outside of the standard reporting timeframe, an out of session report can be provided to the members.

ACT Health Directorate

4.15 The *ACT Health Directorate Strategic Security Governance Arrangements* document outlines the directorate's governance and administrative arrangements for protective security.

4.16 The Health Directorate Security Committee has responsibility for the oversight of protective security in the Health Directorate. Membership includes the Executive Director Business Services, Chief Health Officer, Chief Finance Officer and Executive Directors from the various health services. This committee meets bi-monthly and was in place prior to the introduction of the *ACT Government Protective Security Policy Framework*. The committee reports to the Executive Council and also provides reports to the directorate's Work Health and Safety Committee. It has a standing agenda and clear objectives.

4.17 The Health Directorate protective security governance arrangements are mature, having been in place prior to the *ACT Government Protective Security Policy Framework*. The roles and objectives of the committee are clear: providing strategic support to the implementation of the *ACT Government Protective Security Policy Framework*; monitoring security incidents and discussing emerging issues in the security environment which may impact the ACT Health Directorate in the future.

Education Directorate

4.18 The Security and Emergency Management Committee in the Education Directorate assists the Director-General and Senior Executive to implement the *ACT Government Protective Security Policy Framework* and related security, emergency management, business continuity and related risk management and compliance issues across the directorate.

4.19 The Committee's Terms of Reference establish the governance framework for the Committee and defines its role, responsibilities and authority. The remit of the Committee is broader than just the implementation of the *ACT Government Protective Security Policy Framework*, with the Committee also responsible for emergency management and business continuity.

4.20 The Security and Emergency Management Committee meets four times a year and its members include: the Director, School Improvement; Director, Governance and Community Liaison; Director, Infrastructure and Capital Works; Senior Manager, Internal Audit and Risk Management; Senior Manager, Infrastructure and Capital Works; Agency Security Adviser; Senior Manager, Security and Emergency Management Branch, Justice and Community Safety Directorate; and Manager, ACT Emergency Services Agency. The Security and Emergency Management Committee is co-chaired by the Director, Infrastructure and Capital Works and the Director, Governance and Community Liaison. The directorate advises that this 'allows both areas to jointly plan, strategic, tactical and operational activities'.

Cultural Facilities Corporation

4.21 The Cultural Facilities Corporation *Protective Security Policy and Governance* policy document was developed in September 2017 and outlines the governance and administrative arrangements in place for protective security. The Cultural Facilities Corporation *Protective Security Policy and Governance* document identifies that:

> The Cultural Facilities Corporation Security Executive Group is responsible to the CEO for the ongoing development of the Cultural Facilities Corporation Protective Security policy and Governance and oversight of protective security matters within the Cultural Facilities Corporation.

4.22 In addition, the newly formed Cultural Facilities Corporation Security Executive Group is:

> Responsible for developing a framework of security communications, awareness and training programs to support an informed and aware protective security culture.

4.23 The governance arrangements in the Cultural Facilities Corporation were found to be suitable. The role of the newly established Cultural Facilities Corporation Security Executive Group had yet to be formalised at the time of fieldwork, although the Cultural Facilities Corporation advised that this has since taken place. the Group had not yet met and governance arrangements have not yet been put in place to monitor and report on progress against these responsibilities.

Summary

4.24 All directorates and agencies reviewed as part of this audit have appropriate governance processes in place for the oversight of agency security requirements. Both the Health Directorate and the Education Directorate have established senior management security committees with a focus on security and emergency management issues, noting that for the Cultural Facilities Corporation, the Security Executive Group has only recently been established. For the Chief Minister, Treasury and Economic Development Directorate, it is the Senior Executive Management Group that considers protective security issues.

Directorate and agency policies and procedures

4.25 The *ACT Government Protective Security Policy Framework* mandatory physical security condition PHYSEC 1 requires directorates and agencies to develop and implement directorate and agency-specific protective security policies and procedures that meet their business needs. Each directorate or agency included in the audit had developed policies and procedures that reflected the *ACT Government Protective Security Policy Framework* and provided guidance to agency staff on the implementation of physical security requirements.

Chief Minister, Treasury and Economic Development Directorate

4.26 The Chief Minister, Treasury and Economic Development Directorate developed a *Protective Security Policy and Governance* document in 2015 and this has since been updated in 2017 to reflect the new *ACT Government Protective Security Policy Framework*. This document applies to all Chief Minister, Treasury and Economic Development Directorate business units including Access Canberra and Venues Canberra.

4.27 The policy statement is as follows:

> In support of the ACT Government Protective Security Policy Framework, Chief Minister, Treasury and Economic Development Directorate will establish protective security objectives and employ protective security measures aimed at safeguarding its capabilities and objectives.
>
> Managing security risk is the responsibility of all Chief Minister, Treasury and Economic Development Directorate personnel. Chief Minister, Treasury and Economic Development Directorate personnel and external service providers are to comply with the Chief Minister, Treasury and Economic Development Directorate protective security policies, the ACT Government PSPF and the Commonwealth Information Security Manual (as relevant).

4.28 The *Protective Security Policy and Governance* document outlines the directorate's protective security objectives, governance and administrative arrangements, risk management arrangements and performance monitoring and compliance activities. The document and related guides and forms are available to all staff via the directorate's Security intranet page. The directorate's Security intranet page provides consolidated guidance for staff to access key contact details for the Agency Security Advisers and Agency Security Officers as well as topic-specific policies and procedures.

4.29 In such a diverse directorate, a single Directorate level procedure is unable to capture the nuances of the different types of services and activities of the directorate, which often outside of a standard office environment. As such, the Chief Minister, Treasury and Economic Development Directorate documents provide the framework for business units to develop activity and site-specific procedures, as required, in alignment with directorate-level policies and procedures.

Venues Canberra

4.30 Venues Canberra has developed a Security Plan for each venue, which contains specific information for each site including an alcohol management plan, traffic management plan, and a security brief. These form the operational procedures at each venue.

4.31 Security staff are subcontracted for events. There are deployment plans, operational procedures, training and briefing protocols for contracted security provider staff including:

- formal venue specific training;
- start of shift briefings;
- event specific briefings; and
- change environment briefings.

4.32 These documents also include roles, duties and protocols specific to event at each site.

Access Canberra

4.33 In addition to the overarching Chief Minister, Treasury and Economic Development Directorate policies and procedures, Access Canberra has developed the following business-specific protective security procedures:

- *Security Procedure – Dealing with Aggressive/Threatening Customers*; and
- *Security Procedure - Access Canberra Shopfront Armed Robbery*.

4.34 The Service Centre security procedures are located in the internal knowledge base which all staff have access to. They are reviewed if ever there is an incident and or in line with training. Any changes are approved by the agency security manager before implementation.

4.35 The Contact Centre team has access to documents through either the internal knowledge database or through the intranet within the Contact Centre. They are reviewed and updated regularly as needed. The Contact Centre currently has a draft threat procedure which is being reviewed and updated and once completed will be available through the above.

4.36 In November 2017 Access Canberra engaged a consultant to develop an *Emergency Procedures Manual* for each of its sites. The manuals that were produced are comprehensive documents covering fire evacuation, bomb threats and other emergencies including chemical and medical emergencies. The manuals discuss the roles and responsibilities of the emergency management and emergency control committee for each site, which includes the Chief Wardens, Deputy Wardens and First Aid Officers, as well as checklists and templates. Evacuation diagrams have also been developed.

4.37 Access Canberra has also developed the *Access Canberra Emergency Management and Recovery Plan 2016-18*, which can be activated for an event that impacts directly on Access Canberra/Chief Minister, Treasury and Economic Development Directorate or impacts on the ACT community and requires Access Canberra assistance. The Plan:

> … provides a framework for a response by Access Canberra to any critical incident that affects the ability of the ACT Government to deliver services across a range of business areas. It outlines the control and oversight of mechanisms to be adopted by Access Canberra and the Directorate in the response to, or recovery from, a critical incident following a request from the Emergency Services Agency (ESA) or other lead ACT Government agency, as appropriate.

Health Directorate

4.38 The Health Directorate has developed an *ACT Health Protective Security Policy*. The policy establishes a framework to identify and effectively manage security risks to individuals, property and equipment in ACT Health facilities. The *ACT Health Protective Security Policy* is an integrated policy encompassing the four pillars of security as defined in the *ACT Government Protective Security Policy Framework*. The policy is supported by related procedures and guidelines such as the *Closed Circuit Television Policy* and *Security Design Principles for ACT Health Facilities* document.

4.39 The *ACT Health Protective Security Policy* references the *ACT Government Protective Security Policy Framework* and sets out roles and responsibilities and provides information in relation to each of the four pillars, including diagrams, to indicate the interconnection between documents. The policy provides a mandate for the development of protective security plans and procedures and the implementation and monitoring of controls to effectively manage security risk.

4.40 In addition, the Health Directorate has a range of standard operating procedures to support physical security within and around its facilities. These are available to all Health Directorate employees by accessing the policy register on the Health Directorate intranet. Some apply to all locations, while others are specific to the location and health services provided. Examples of the documentation available included:

- *Closed Circuit Television Policy* and *Closed Circuit Television Request form* – this document provides ACT Health staff and contractors direction on their obligations in relation to the use, managing, monitoring, recording, duplication, data storage, release and general access of CCTV systems;
- responses to the various security codes, for example, *Code Black Personal Threat Procedure* – this procedure mitigates the risk of occurrence of a code-black (personal threat), when it is appropriate to call a code-black as well as how to call, respond to and report a code-black;
- *Use of Duress alarms in AMHU Procedures* – this procedure provides for staff to be properly equipped with duress alarms and to understand the proper usage and response to a duress alarm; and

- *Staff Identification Procedure* – this is a procedures for the provision of access cards, including the colour coding used to differentiate staff (admin, allied health, medical, security).

4.41 It was noted that some of the standard operating procedures were last updated in 2012, for example the policies for the use of duress alarms in both the Alcohol and Drug Services and the Adult Mental Health Unit. These should be reviewed to ensure that they are current.

4.42 The Health Directorate works within existing standard health industry security management processes including standard alert codes. The code system is used across all Health Directorate facilities. Each code has an *Emergency Response Plan* that is commensurate with the risk level and type of incident. For easy access, these codes are attached to every staff member's access card and a one-page *Emergency Procedures Canberra Hospital* infogram has been developed, which provides further guidance on the different codes (and colour coding) and actions to manage.

4.43 Within the Directorate there are also procedures that are specific to a particular site, to take into account unique features such as the services offered and the client profile as well as the building features. For example, there are two new buildings, the Dhulwa Mental Health Unit and Belconnen Health Centre, with security considerations taken into account at the design phase, which have site-specific protocols based on their client profile.

4.44 The Health Directorate is currently drafting a *Protective Security Strategy 2018-2023* (the Strategy) in line with the revised 2017 *ACT Government Protective Security Policy Framework*. The purpose of the Strategy is to ensure that the Health Directorate delivers a consistent and consolidated approach to promoting the management of security practices and infrastructure. The intent of the *Protective Security Strategy 2018-2023* is to articulate the Health Directorate's strategic focus for protective security across the directorate for the next five years to consolidate current activities and provide a focus going forward.

4.45 The *Security Design Principles for ACT Health Facilities* applies the *ACT Government Protective Security Policy Framework* Security Zone Classification System to indicate the requirements based on the zone, enabling a consistent risk based approach to be taken. This includes controls such as:

- Perimeter security including fencing, CCTV, bollards including the impact of vegetation and landscaping on the effectiveness of these;
- Access control systems (EACS) and mechanical keys;
- Access doors and lockdown requirements;
- Intruder detection - reed switches;
- Duress alarms; and
- Visitor management.

4.46 Ideally, security requirements are considered at the initial design phase of a building or re-modelling project, enabling physical security features to be incorporated into the building. The *Security Design Principles for ACT Health Facilities* (March 2017) document provides:

> Information for briefing architects and consultants and commissioning planners for all Health and Capital Upgrades Program (CUP) projects.

4.47 In regard to any infrastructure upgrade or build, plans will be provided to the Health Directorate security team to assess. The focus is to embed security into any build, such as passive security design. Examples of this include high/wide counters rather than glass partitions, providing a less intrusive barrier, and ensuring that consulting rooms have two exits.

Education Directorate

4.48 The *ACT Education Directorate Security Management Policy* identifies protective security as a core element of the Education Directorate's planning and approval processes and supports the implementation of the *ACT Government Protective Security Policy Framework*. The security policy and associated procedures establishes the Education Directorate's expectations regarding the management of security risk.

4.49 The Security Management Policy states that:

> The Directorate's responsibility under the Framework is to establish policies and procedures to protect ACT Government employees, clients, assets and information, and ensure the Directorate manages protective security in a consistent manner.

Emergency management

4.50 The Education Directorate has in place extensive emergency management policies and procedures covering internal school or office-based incidents or emergencies as well as external emergencies that impact schools. The *ACT Education Emergency Management Framework*, the *Emergency Support Team Network*, the *Temporary Closure of Schools* policy and associated procedure, and other policies and procedures identify key roles and responsibilities and processes to be followed to enable the Education Directorate to activate these procedures and work with external directorates/agencies.

School Management Manual

4.51 The *ACT Education and Training School Management Manual* has a chapter specifically covering security and emergency management. The Manual aligns with the *Security Management Policy* and the *Emergency Planning and Fire Safety Policy* which in turn align with the *ACT Government Protective Security Policy Framework* and other policies and legislation.

4.52 The *ACT Education and Training School Management Manual* details physical security measures that schools must follow, related actions that are the responsibility of the school and the process for security incident reporting.

4.53 In addition, schools are required to complete an end of term checklist to ensure that school sites, assets and resources are secure prior to the school holiday periods. This checklist is designed to confirm that the physical security measures in place are fully operational. This is signed by the school Business Manager and Principal and placed on a school based file. It is noted that a copy of this document is not provided to the Education Support Office for confirmation or review.

Excursions

4.54 In the Education Directorate, school-based staff and students are involved in excursions, local, interstate and international, and as a result physical security risks need to be considered in other contexts. The Education Directorate has established an *Education Directorate Excursion Policy* and *Education Directorate Overseas Excursion Policy* as well as associated procedures, templates and other guidance to ensure the safe conduct and management of excursions.

4.55 A key process for school excursions is the conduct of a risk assessment, and where relevant, emergency planning. This component of the relevant excursion forms and templates seeks to identify risks and promote the identification and implementation of controls to mitigate the risk. In some instances, the risks cannot be sufficiently mitigated and proposed excursion activities need to be amended. Excursions with a high risk, including overseas and outdoor education excursions, need additional approvals to ensure all risks have been identified and mitigated, noting that some activities and countries are excluded. The Education Directorate advised that all risk assessments for excursions are reviewed by the Internal Audit and Risk Management Section and all emergency management plans for overseas school excursions are also reviewed by the Internal Audit and Risk Management Section.

Protection from occupational violence

4.56 The Education Directorate seeks to implement policies and procedures so that Canberra public schools are safe, respectful and supportive learning and teaching communities that promote student and staff wellbeing. To support this, the Directorate has in place the following core policies:

- *Managing Occupational Violence Policy* commits the Directorate to protect staff in the course of their work from exposure to occupational violence risk and to clearly demonstrate that occupational violence is unacceptable; and
- *Safe and Supportive Schools Policy* commits the Directorate to supporting principals to create, and maintain a safe, respectful and supportive school environment that fosters safety and the wellbeing of students and staff.

4.57 These policies are available on the intranet and reference related policies and documents. In addition, there are procedures, factsheets, and risk management documentation to support these policies.

Cultural Facilities Corporation

4.58 The Cultural Facilities Corporation has in place a *Cultural Facilities Corporation Protective Security Policy and Governance* policy document that was signed off on 15 September 2017 in support of the *ACT Government Protective Security Policy Framework*. Based on the *ACT Government Protective Security Policy Framework*, this policy provides the governance framework for a systematic and coordinated approach to security risk management by Cultural Facilities Corporation personnel and external service providers under contract. In addition, current site security procedures can be ramped up based on an assessment of risk, such as a controversial performer at the Canberra Theatre or a mass gathering at one of the historic places.

4.59 The *Protective Security Policy and Governance* policy document provides an overview of security governance, security risk management and planning, performance monitoring and compliance. It sets out the Cultural Facilities Corporation's protective security objectives, which are to:

- protect staff, contractors and visitors from harm;
- protect Cultural Facilities Corporation information, assets and infrastructure against unauthorised access, sabotage, wilful damage, theft or disruption;
- protect assets and other materials left in trust with the Cultural Facilities Corporation from harm; and
- protect the information and assets of other directorates and directorates/agencies and other jurisdictions in accordance with security agreements and obligations between Cultural Facilities Corporation and those other directorates, directorates/agencies and jurisdictions.

4.60 The document also outlines the protective security responsibilities of key stakeholders within the Cultural Facilities Corporation and the high level responsibilities of the Agency Security Executive Group who are responsible for developing a framework of security communications, including the Cultural Facilities Corporation security plan, awareness and training programs throughout the Cultural Facilities Corporation to support an informed and aware protective security culture.

Training and support

Chief Minister, Treasury and Economic Development Directorate

4.61 The Chief Minister, Treasury and Economic Development Directorate Security intranet page includes the *Protective Security Policy Framework* e-animation training package, which was developed by the Security and Emergency Management Branch, and six other training packages which cover other related topics.

4.62 The intranet page also includes a *Security Awareness Training Guide*, which provides details on what should be addressed in training packages dealing with identifying and managing security threats or incidents. The Guide suggests that protective security should be included as part of new employee induction and that training to all staff could be provided via face to face sessions or online.

4.63 Security training is included as part of induction and security training sessions are scheduled in June and December as part of the corporate training calendar, with attendee records maintained. In addition, ad hoc team training can be provided on request to the Agency Security Advisers.

4.64 It is noted that formal training is only one component that can be used to promulgate and educate staff in regards to protective security. While all security information is available on the staff intranet, communications are used by the Agency Security Adviser - Governance through all staff emails and LOOP e-newsletter articles to promote a better understanding of protective security. For example, a security incident factsheet was promulgated via an intranet article in December 2017.

4.65 Staff access the Chief Minister, Treasury and Economic Development Directorate and Access Canberra security training, along with fraud and ethics training, however this training is not mandatory. The Directorate maintains records as to who has attended the training sessions.

Access Canberra

4.66 Access Canberra has engaged an external provider to provide training for dealing with aggressive customers and robbery response. The training is run on demand, generally every three months. While this is primarily for its own staff, other directorates and agencies can also access this training if space allows.

4.67 An orientation checklist is also utilised by Access Canberra to ensure that procedures/protocols have been relayed appropriately to people, including staff, contractors, tradespeople and visitors, prior to commencing work in the service centres. The checklist includes the following items:

- the Health and Safety Representative (HSR) has been identified;
- the reporting procedure for hazards and incidents has been briefly outlined; and
- the Shopfront security arrangements and provisions have been outlined.

4.68 Acknowledging that the high level governance, policies and procedures with direct linkages to the *ACT Government Protective Security Policy Framework* are managed at a directorate level, Access Canberra has training in place to inform its staff of the physical security of their workplaces.

Health Directorate

4.69 The Health Directorate has developed a Protective Security e-learning package. The package is available to all staff but is not compulsory; its mandatory completion is dependent on its relevance to a staff member's role. The Health Directorate has identified improvements that are required to update it to reflect the 2017 version of the *ACT Government Protective Security Policy Framework*. .

4.70 Protective security is also incorporated in a mandatory annual Fire, Emergency and Security e-learning package. This e-learning package is part of the directorate's *Essential Education Policy*, which also includes identifying security systems in place. The Staff Development Unit is responsible for the administration of the Health Directorate's *Essential Education Policy* which is monitored by managers on Capabiliti. As a requirement for accreditation, completion by 95 per cent of staff is required.

4.71 With the exception of the corporate functions, the majority of Health Directorate staff have clinical or specialist training requirements to complete in order to maintain their currency. As protective security is included in the Fire, Emergency and Security e-learning package, and given other training requirements, not mandating the protective security training is appropriate.

Education Directorate

4.72 There is no specific protective security training provided by the Education Directorate. Schools reported that new administrative and teaching staff at the school participate in an on-site induction, which includes physical security protocols. The schools reviewed as part of the audit also have a school guide, which included security protocols and emergency procedures, which is updated at least annually and accessible to all staff.

4.73 The Agency Security Adviser met with some of the Business Services Officers from schools in February 2017 and the Agency Security Adviser and Agency Security Officer recently coordinated meetings with principals and ACT Policing representatives to discuss and increase awareness of protective security issues and trends, including physical security. In the school context, this may provide better outcomes than standard 'training' as discussion points can be transferred to school-based protocols and disseminated to staff. These forums also initiate conversations and linkages between schools managing the same issues, enabling schools to leverage off the experiences of others.

Cultural Facilities Corporation

4.74 Training is an area that is expected to be addressed as part of the implementation of the Cultural Facilities Corporation *Protective Security Policy and Governance* policy document, which was finalised in September 2017. The need for security awareness training was first highlighted in the 2014 Security Risk assessment of the Canberra Theatre:

> Security awareness training should cover the following areas:
>
> - Canberra Theatre security procedures and policies.
> - Personnel safety measures.
> - Asset protection.
> - Behavioural awareness.
> - Access control procedures.

4.75 Since 2014 security awareness training for staff dealing with the public has been undertaken with respect to dealing with difficult clients, and operationally staff are aware of day-to-day security requirements. However, wider security training is being considered as a response to security risk assessments undertaken in 2017.

4.76 As above, it will be the responsibility of the Cultural Facilities Corporation Security Executive Group to strengthen the current framework for training and communications framework, in order to embed a security culture within the Cultural Facilities Corporation.

Incident management and reporting

4.77 Physical security mandatory conditions in the *ACT Government Protective Security Policy Framework* require processes for the reporting of security and work health and safety incidents.

Chief Minister, Treasury and Economic Development Directorate

4.78 The Chief Minister, Treasury and Economic Development Directorate has modified the *Maturity Assessment Tool*, as provided by Security and Emergency Management Branch, for its own internal purposes, to improve monitoring and reporting. It has been modified to compare the Directorate's protective security capability as of October 2016 against its March 2017 capability, in order to track progress over time. The *Maturity Assessment* Tool also provides a target capability for June 2018, and this is expected to provide greater visibility of progress in the implementation of the *ACT Government Protective Security Policy Framework*.

4.79 In addition to Directorate or whole-of-government reporting, the Chief Minister, Treasury and Economic Development Directorate has processes in place to capture security incidents. Following an incident, staff are required to complete a *Security Incident Report* form within 48 hours using the *Security Incident Report* template. The template requires staff to identify the incident as a physical security incident or a protective security breach, and provide

further details on the incident itself as well as follow-up actions. The forms are provided to the Shared Services ICT Protective Security Team via email.

4.80 The Agency Security Adviser (Governance) has access to the security reports and the reporting system Perspective. At the Agency Security Adviser (Governance)'s request, the Shared Services Protective Security Team extract a summary report every six months for analysis and reporting. During the period 1 December 2016 - 30 April 2017, five security incidents were reported across the Chief Minister, Treasury and Economic Development Directorate: three reported disruptive persons; one suspicious activity; and one theft were reported for the period. As discussed previously, the summary of security incidents is reported to the Executive Management Group.

4.81 In Access Canberra security and work health and safety incidents are reported using Chief Minister, Treasury and Economic Development Directorate processes. Following an incident in an Access Canberra shopfront, a report will be provided to the Senior Manager Access Canberra service centres using RiskMan (Risk Management software). This is provided to the Chief Minister, Treasury and Economic Development Directorate Agency Security Advisers and escalated to the Deputy Director-General.

Health Directorate

4.82 In the Health Directorate incidents are reported in the RiskMan system (risk management software), which collects both clinical and staff incidents and 'near misses'. The Health Directorate Security Committee receives reporting of themes and subsequent actions in the form of the *Protective Security Report* at each quarterly meeting. The *Protective Security Report* is also provided to the OHS Committee and Quality and Safety Committee. The Directorate is investigating options to improve the system to enable reporting at a more granular level. This includes a solution to allow security to report incidents as they occur.

Education Directorate

4.83 The Education Directorate has a framework of policies and supporting documentation in relation to reporting, managing and supporting staff and students during critical and non-critical incidents.

4.84 In the Education Directorate critical incidents are monitored and reported on via a daily critical incident reporting email, which goes to the Education Directorate's senior executive, in addition to immediate notifications to those with responsibilities for support and management.

4.85 The individual critical incident reports are summarised into a quarterly report for behavioural incidents and a quarterly report for infrastructure security issues. The Directorate's Security Emergency Management Committee receives both of these reports, to discuss trends and preventative actions.

4.86 Depending on the incident there may be a requirement to complete additional reporting such as a student accident report, a notifiable incident under Work Health and Safety laws in the RiskMan system (risk management software), or mandatory reporting if child abuse is suspected.

4.87 Most incidents that occur in schools are classified as non-critical. A non-critical incident is defined as:

> An event which is unanticipated or outside the accepted social norm, but which, in the experience of the general community, would not be considered an extraordinary occurrence or situation, and which the school has strategies and procedures in place to manage with little or no external assistance.

4.88 However, critical incidents involving the school premises, staff, students and visitors do occur. A critical or emergency incident is defined as follows:

> An event that causes severe impact, such as significant disruption to the school routine, an emergency management situation, or threat to the safety of students and staff.

Cultural Facilities Corporation

4.89 As per the Cultural Facilities Corporation *Protective Security Policy and Governance* policy document:

> The Agency Security Executive Group will also provide an annual assessment of the overall state of Cultural Facilities Corporation security performance to the CEO. This will outline, amongst other things:
>
> - The Cultural Facilities Corporation's compliance status against the ACT Government PSPF;
> - Analysis of security incident reporting and the results of security investigations; …

4.90 Incidents, including security incidents, require employees to complete a form in the RiskMan system (risk management software). This includes near-misses, violent incidents and injuries.

4.91 The Cultural Facilities Corporation has an *ACT Historic Places Incident Response Procedures* document which provides first response procedures for staff and volunteers at the ACT Historic Places sites at Lanyon Homestead, Calthorpes' House and Mugga Mugga Homestead. The aim is to ensure appropriate, effective and timely response to any significant incident that occurs at one of the sites managed by ACT Historic Places. Incident reporting procedures include following work health and safety reporting procedures (that is, reporting the incident in RiskMan).

Summary

4.92 All directorates and agencies have incident reporting procedures in place that include reporting work health and safety incidents and near misses in RiskMan. Furthermore, all directorates and agencies have identified processes to report periodically on incidents and enable them to analyse incident data for specific risks or recurring themes.

Compliance with the *ACT Government Protective Security Policy Framework*

Audit Office assessment

4.93 Meehan & Meehan Pty Ltd was engaged by the ACT Audit Office to conduct physical security site assessments across a selection of agency sites during November 2017 for:

- Chief Minister, Treasury and Economic Development Directorate – Venues Canberra;
- Chief Minister, Treasury and Economic Development Directorate – Access Canberra;
- ACT Health Directorate;
- Education Directorate; and
- Cultural Facilities Corporation.

4.94 The site inspections included discussions with managers with responsibility for day-to-day operations and site management as well as an assessment of the suitability of the physical security controls in place.

4.95 To meet requirements of the four physical security mandatory conditions (refer to paragraph 1.6) the agency was expected to have in place:

- a physical security policy and plan;
- evidence of integration of protective security in design and modification of facilities, including consideration of Work Health and Safety obligations; and
- evidence of duty of care considerations for the public accessing services.

4.96 As part of the audit, site-specific security risk assessments were conducted by the subject matter expert to assess the implementation of physical security practices and controls across a sample of sites.

4.97 Details of the results of the site-specific security risk assessments were provided to the relevant directorates and agencies.

Chief Minister, Treasury and Economic Development Directorate

4.98 The Meehan and Meehan Pty Ltd report provided to the Audit Office stated:

> Chief Minister, Treasury and Economic Development Directorate demonstrated a developing security culture. The Directorate combines a number of dissimilar business units which portrayed varying degrees of maturity of analysis, planning and control implementation. Both Venues Canberra and Access Canberra: … have sound engagement with security risk, effective controls and well-developed doctrine.

Venues Canberra

4.99 The results of the Meehan and Meehan Pty Ltd review of Venues Canberra sites against the four physical security mandatory requirements of the *ACT Government Protective Security Policy Framework* noted that for Venues Canberra:

> … security and emergency management plans require further description of the authority and obligations of "Person Conducting the Business" in relation to [work health and safety] obligations and that person's relationship to managing security risk.
>
> … risk assessments and planning documentation demonstrated an understanding of their duty of care to provide safety for … members of the public … some policy or procedural content may need review ...

4.100 According to Meehan and Meehan Pty Ltd Venues Canberra sites have effectively implemented physical security policies, procedures and controls to ensure the physical safety of employees and members of the public but require separation of security and emergency management planning to achieve full compliance with governance and physical security requirements of the *ACT Government Protective Security Policy Framework*.

Access Canberra

4.101 The results of the Meehan and Meehan Pty Ltd review of Access Canberra sites against the four physical security mandatory requirements of the *ACT Government Protective Security Policy Framework* noted that Access Canberra:

> … security and emergency management plans require further description of the authority and obligations of "Person Conducting the Business" in relation to [work health and safety] obligations and that person's relationship to managing security risk.
>
> … risk assessments and planning documentation demonstrated an understanding of their duty of care to provide safety for … members of the public … some policy or procedural content may need review …

4.102 According to Meehan and Meehan Pty Ltd overall the Access Canberra sites had sound engagement with security risk, effective controls and well-developed doctrine.

Health Directorate

4.103 In relation to the Health Directorate overall, the Meehan and Meehan Pty Ltd report found:

> Sites inspected within the Health Directorate have effectively implemented physical security policies, procedures and controls to ensure the physical safety of employees and members of the public. These sites are rated as fully effective against the audited governance and physical security requirements of the 2014 PSPF.

4.104 In relation to the Health Directorate sites considered as part of the audit, the Meehan and Meehan Pty Ltd report stated:

> Inspection sites … within the ACT Health Directorate demonstrated a mature security risk culture with comprehensive risk analysis and well-defined security role player functions and responsibilities.
>
> Health provided exemplars for ACT Government physical security risk management.

4.105 According to Meehan and Meehan Pty Ltd the Health Directorate had effective protective security control elements in place at all sites assessed as part of the audit to manage the physical security of people, information and assets commensurate with the level of risk.

Education Directorate

4.106 In relation to the Education Directorate's physical security at the sites considered as part of the audit, the Meehan and Meehan Pty Ltd report stated:

> Education Directorate has effectively implemented physical security policies, procedures and controls to ensure the physical safety of students, employees and members of the public, however requires a separation of protective security risk and the development of security risk assessments and plans to achieve full compliance with governance and physical security requirements of the PSPF.

4.107 Current physical security control elements were assessed as adequate, with the Meehan and Meehan Pty Ltd report stating:

> All have effectively implemented physical security policies, procedures and controls to ensure the physical safety of students, employees and members of the public.

4.108 Overall, the Meehan and Meehan Pty Ltd report found:

> Sites audited in ACT Education Directorate demonstrated a maturing security culture with centralised risk analysis, plan development, control procurement and implementation. Education Directorate has an agency wide protective security policy; however, security risk identification and management are contained within its emergency management planning framework. Education Directorate has effectively implemented physical security policies, procedures and controls to ensure the physical safety of students, employees and members of the public.

4.109 The report found that physical security is included as part of the design and planning of new schools. However, it was noted that a standard approach cannot be taken due to building limitations and community feedback impacting on control elements. School physical security risk profiles can change dependent on the cohort of students and parents as well as national and international events. As such, the risk profile needs to be monitored and additional mechanisms implemented as required.

Cultural Facilities Corporation

4.110 The results of the review of the Cultural Facilities Corporation sites against the four physical security mandatory requirements in the *ACT Government Protective Security Policy Framework* found that the Cultural Facilities Corporation:

> … did not provide a [whole-of-agency protective security policy] which provides mandate to risk assess and implement controls to manage security related risks. Some security related risks were addressed in emergency management plans and response procedures …
>
> … security and emergency management plans require further description of the authority and obligations of "Person Conducting the Business" in relation to [work health and safety] obligations and that person's relationship to managing security risk.
>
> … risk assessments and planning documentation demonstrated an understanding of their duty of care to provide safety for … members of the public … some policy or procedural content may need review ...

Audit reports

Reports Published in 2017-18	
Report No. 05 – 2018	ACT clubs' community contributions
Report No. 04 – 2018	2016-17 Financial Audits – Computer Information Systems
Report No. 03 – 2018	Tender for the sale of Block 30 (formerly Block 20) Section 34 Dickson
Report No. 02 – 2018	ACT Government strategic and accountability indicators
Report No. 01 – 2018	Acceptance of Stormwater Assets
Report No. 11 – 2017	2016-17 Financial Audits – Financial Results and Audit Findings
Report No. 10 – 2017	2016-17 Financial Audits – Overview
Report No. 09 – 2017	Annual Report 2016-17
Report No. 08 – 2017	Selected ACT Government agencies' management of Public Art
Reports Published in 2016-17	
Report No. 07 – 2017	Public Housing Renewal Program
Report No. 06 – 2017	Mental Health Services – Transition from Acute Care
Report No. 05 – 2017	Maintenance of Selected Road Infrastructure Assets
Report No. 04 – 2017	Performance information in ACT public schools
Report No. 03 – 2017	2015-16 Financial Audits – Computer Information Systems
Report No. 02 – 2017	2016 ACT Election
Report No. 01 – 2017	WorkSafe ACT's management of its regulatory responsibilities for the demolition of loose-fill asbestos contaminated houses
Report No. 11 – 2016	2015-16 Financial Audits – Financial Results and Audit Findings
Report No. 10 – 2016	2015-16 Financial Audits – Audit Reports
Report No. 09 – 2016	Commissioner for International Engagement – Position Creation and Appointment Process
Report No. 08 – 2016	Annual Report 2015-16
Report No. 07 – 2016	Certain Land Development Agency Acquisitions
Reports Published in 2015-16	
Report No. 06 – 2016	Management and administration of credit cards by ACT Government entities
Report No. 05 – 2016	Initiation of the Light Rail Project
Report No. 04 – 2016	The management of the financial arrangements for the delivery of the Loose-fill Asbestos (Mr Fluffy) Insulation Eradication Scheme
Report No. 03 – 2016	ACT Policing Arrangement
Report No. 02 – 2016	Maintenance of Public Housing
Report No. 01 – 2016	Calvary Public Hospital Financial and Performance Reporting and Management
Report No. 10 – 2015	2014-15 Financial Audits
Report No. 09 – 2015	Public Transport: The Frequent Network
Report No. 08 – 2015	Annual Report 2014-15
Reports Published in 2015	
Report No. 07 – 2015	Sale of ACTTAB
Report No. 06 – 2015	Bulk Water Alliance
Report No. 05 – 2015	Integrity of Data in the Health Directorate
Report No. 04 – 2015	ACT Government support to the University of Canberra for affordable student accommodation

These and earlier reports can be obtained from the ACT Audit Office's website at http://www.audit.act.gov.au.