

VAGO

Victorian Auditor-General's Office



ICT Disaster Recovery Planning

November 2017



ICT Disaster Recovery Planning

Ordered to be published

VICTORIAN GOVERNMENT PRINTER

November 2017

PP No 262, Session 2014–17

This report is printed on Monza Recycled paper. Monza Recycled is certified Carbon Neutral by The Carbon Reduction Institute (CRI) in accordance with the global Greenhouse Gas Protocol and ISO 14040 framework. The Lifecycle Analysis for Monza Recycled is cradle to grave including Scopes 1, 2 and 3. It has FSC Mix Certification combined with 55% recycled content.

ISBN 978 1 925678 04 8



The Hon Bruce Atkinson MLC
President
Legislative Council
Parliament House
Melbourne

The Hon Colin Brooks MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit my report
ICT Disaster Recovery Planning.

Yours faithfully

A handwritten signature in black ink, appearing to read "Andrew Greaves", with a long horizontal stroke extending to the right.

Andrew Greaves
Auditor-General

29 November 2017

Contents

Audit overview	7
Conclusion.....	8
Findings.....	8
Recommendations	15
Responses to recommendations.....	17
1 Audit context	19
1.1 ICT disaster recovery	19
1.2 ICT asset management	23
1.3 Legislation and standards.....	24
1.4 Why this audit is important.....	25
1.5 Previous audits	26
1.6 What this audit examined and how	26
1.7 Report structure	27
2 Department of Economic Development, Jobs, Transport and Resources	29
2.1 Business impact analysis	29
2.2 Disaster recovery.....	31
2.3 Obsolescence in systems	34
3 Department of Environment, Land, Water and Planning.....	37
3.1 Business impact analysis	37
3.2 Disaster recovery.....	39
3.3 Obsolescence in systems	42
4 Department of Health and Human Services	45
4.1 Business impact analysis	45
4.2 Disaster recovery.....	47
4.3 Obsolescence in systems	51
5 Department of Justice and Regulation	53
5.1 Business impact analysis	53
5.2 Disaster recovery.....	55
5.3 Obsolescence in systems	58
6 Victoria Police	59
6.1 Business impact analysis	59
6.2 Disaster recovery.....	62
6.3 Obsolescence in systems	64

Appendix A. <i>Audit Act 1994</i> section 16—submissions and comments	65
---	----

Appendix B. Capability levels and descriptions.....	81
---	----

Acronyms

AMAF	Asset Management Accountability Framework
ANAO	Australian National Audit Office
BIA	Business impact analysis
DEDJTR	Department of Economic Development, Jobs, Transport and Resources
DELWP	Department of Environment, Land, Water and Planning
DHHS	Department of Health and Human Services
DJR	Department of Justice and Regulation
DRP	Disaster recovery plan
DTF	Department of Treasury and Finance
ICT	Information and communications technology
VAGO	Victorian Auditor-General's Office
VGRMF	Victorian Government Risk Management Framework
VPDSF	Victorian Protective Data Security Framework
VPDSS	Victorian Protective Data Security Standards

Audit overview

Information and communications technology (ICT) systems are critical for the operations of government agencies. Agencies depend on them to:

- deliver public services—including essential services—to the community
- efficiently and effectively manage operations
- fulfil their statutory obligations.

To make sure their systems remain available and continue to operate reliably, agencies must be able to recover and restore them in the event of a disruption—such as an event that interrupts access to premises, to the data that systems rely on, or to the systems themselves. Further, agencies need to be able to recover and restore their systems within a time frame that reflects the business-critical nature of each system.

ICT disaster recovery is the process for recovering systems following a major disruption. ICT disaster recovery planning forms part of an agency's wider business continuity strategy.

Managing disaster recovery risk presents special challenges. The likelihood of a major disaster or significant disruption is generally low, often remote—but the consequences of a system failure that cannot be restored could be significant or even catastrophic.

Without effective disaster recovery capability, agencies risk:

- extended disruption or inability to deliver public services that depend on systems
- inability to recover systems and restore lost data
- subsequent financial loss to themselves and the Victorian economy
- reputational damage, including loss of community confidence in the effective delivery of government services.

Agencies can reduce the likelihood of disruption events, however this approach can require significant investment compared to the direct costs of responding to a disruption when it occurs. It can therefore be challenging for agencies to determine the balance between focusing on preventative actions and planning to manage the consequences of possible disruptions.

In this audit, we examined disaster recovery at Victoria Police and four departments that provide essential government services—the Department of Economic Development, Jobs, Transport and Resources (DEDJTR), the Department of Environment, Land, Water and Planning (DELWP), the Department of Health and Human Services (DHHS) and the Department of Justice and Regulation (DJR).

We assessed whether their ICT disaster recovery processes are likely to be effective in the event of a disruption.

Conclusion

At present, none of the agencies we audited have sufficient assurance that they can recover and restore all of their critical systems to meet business requirements in the event of a disruption.

They do not have sufficient and necessary processes to identify, plan and recover their systems following a disruption. Compounding this is the relatively high number of obsolete ICT systems all agencies are still using to deliver some of their critical business functions. This both increases the likelihood of disruptions through hardware and software failure or external attack, and makes recovery more difficult and costly. These circumstances place critical business functions and the continued delivery of public services at an unacceptably high risk should a disruption occur.

Agencies are only just beginning to fully understand the importance of comprehensively identifying and prioritising their business functions, maintaining the ICT systems that support these functions, and establishing recovery arrangements to maintain continuity of service.

They need to significantly improve and develop well-resourced and established processes that fully account for and can efficiently recover the critical business functions of agencies following a disruption.

Findings

Business impact analysis







None of the agencies' business impact analysis (BIA) processes are robust enough to identify and prioritise critical business functions and the recovery requirements for related ICT systems. The maturity of agencies' processes varies, and there are several common weaknesses:

- not all business functions and related ICT systems are clearly identified and prioritised
- systems' recovery requirements are only assessed in isolation, and system dependency requirements are not identified and considered
- systems' recovery requirements determined by the business have not been aligned with ICT service delivery and system recovery capabilities.

Agencies are either not performing BIA periodically, or their BIA does not have defined trigger events that prompt them to revise the analysis in response to changes at the agency—for example, a different operating environment, new services or an altered risk profile.

We measured agencies' BIA processes against the globally accepted model outlined in *COBIT Process Assessment Model: Using COBIT 5*, 2013 (the COBIT 5 model). This model assesses the capability of the processes using the scale shown in Figure A.

Figure A
COBIT 5 capability levels and descriptions

Capability level	Description
 Incomplete	Process is not in place or cannot achieve its objective
 Performed	Process is in place and achieves its purpose
 Managed	Process is implemented in a managed way and appropriately controlled and maintained
 Established	Process is implemented using a defined process that is capable of achieving its outcomes
 Predictable	Process operates consistently within defined limits to achieve its outcomes
 Optimised	Process is continuously improved to meet relevant current and projected enterprise goals

Source: VAGO, based on COBIT 5 ISO/IEC 15504 capability levels.

Figure B shows our assessment of the capability of the agencies' BIA processes.

Figure B
Capability of audited agencies' BIA process

Criterion	DEDJTR	DELWP	DHHS	DJR	Victoria Police
BIA process					

Source: VAGO.

Without a robust BIA, agencies have difficulty determining which systems need disaster recovery capability and in what order they should recover systems. The immaturity of these BIA processes means agencies risk not being able to identify all the systems that support their critical business functions. Further, they risk not having the necessary disaster recovery capability to ensure that their ICT systems can provide continuous service or be recovered rapidly following a disruption.

In this report, our assessment is based on the critical systems that agencies have identified.

Disaster recovery processes

None of the agencies' disaster recovery processes are robust enough to effectively and efficiently recover all critical systems in the event of a disruption. Agencies' disaster recovery processes show similar degrees of capability.

We used the COBIT 5 model to assess agencies' disaster recovery processes, as shown in Figure C.

Figure C
Capability of audited agencies' disaster recovery processes



Source: VAGO.

Across all the audited agencies, we identified that disaster recovery processes require improvement:

- Agencies do not have an established, coordinated department-wide approach to ICT disaster recovery planning—instead, management of disaster recovery is decentralised and managed by individual business divisions.
- Not all systems that support critical business functions have disaster recovery plans (84 out of 222 systems). Agencies have not performed a risk assessment to determine which critical systems need a disaster recovery plan or identified appropriate continuity processes for when systems are unavailable.

Disaster recovery testing

No agency is performing functional disaster recovery tests for all systems that support critical business functions and, when agencies do conduct testing, they are not performing it consistently.

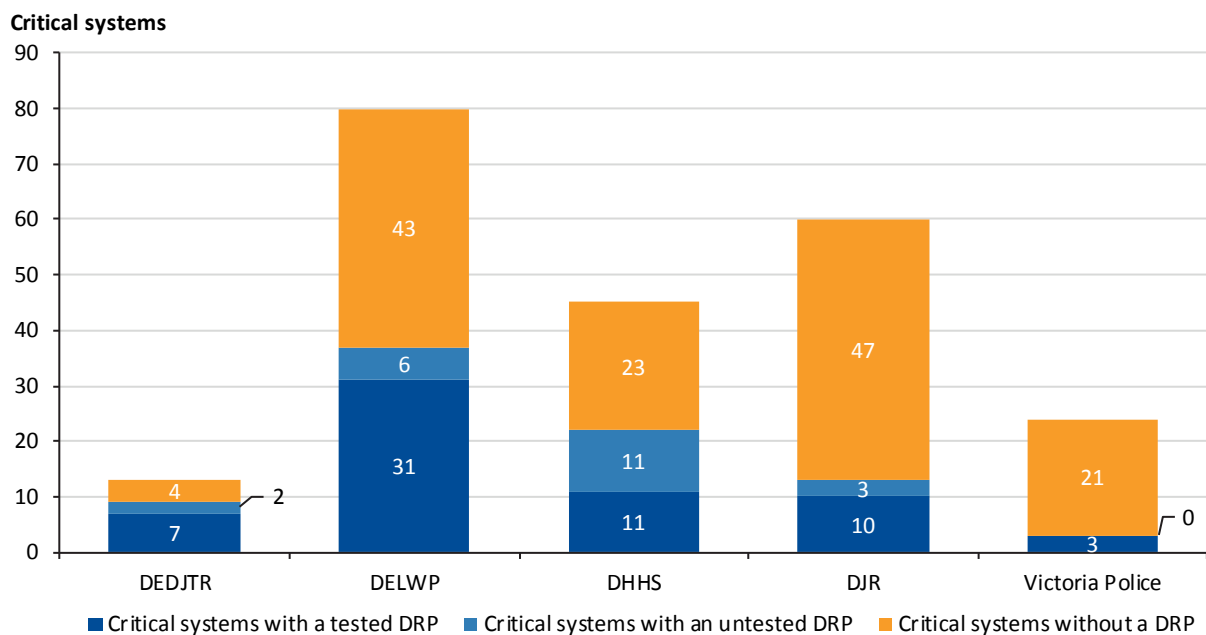
No agencies' functional disaster recovery testing verifies whether the agency can recover systems to meet the two key recovery objectives:

- **recovery time**—the target time required for the recovery of an ICT system after a disruption
- **recovery point**—the point in time to which an agency must restore data after a disruption, for example, restoring data to the end of the previous day's processing.

The reason why agencies cannot verify whether their systems are able to meet these recovery objectives is because their BIA fails to determine them.

Figure D shows the number of disaster recovery plans agencies have developed and tested for the systems that support critical business functions. Most do not have disaster recovery plans.

Figure D
Critical systems and disaster recovery plans



Note: DRP = disaster recovery plan.

Source: VAGO.

Without having disaster recovery plans and testing them regularly, agencies risk not being able to recover systems in a timely way because of a lack of guidance for staff on what is required to bring systems back online. As a result, critical government services—such as criminal justice and policing operations—may be unavailable for longer than is necessary, depending on the scale of the disruption.

Disaster recovery training

None of the agencies provide enough training to staff with specific disaster recovery roles and responsibilities to equip them with the knowledge and skills needed to manage the recovery of a system after a disruption. Active participation in disaster recovery tests and theoretical training is a key tool for developing staff skills and experience.

Data centre arrangements

Victoria Police hosts its ICT systems in the same building as its operations. There is a risk that disruptions affecting the operational site—such as a fire—will also affect its systems. Victoria Police has other data centre facilities, which can mitigate the risk and provide systems with the required redundancy capability—the duplication of a system to increase its reliability and minimise downtime in the event of disruption.

Victoria Police is currently in the process of relocating its systems to a separate data centre facility, which it expects to complete by 2020. Victoria Police intends to enhance the disaster recovery capability of all critical systems by 31 December 2018, in preparation for the data centre relocation. However, the risk will remain until then.

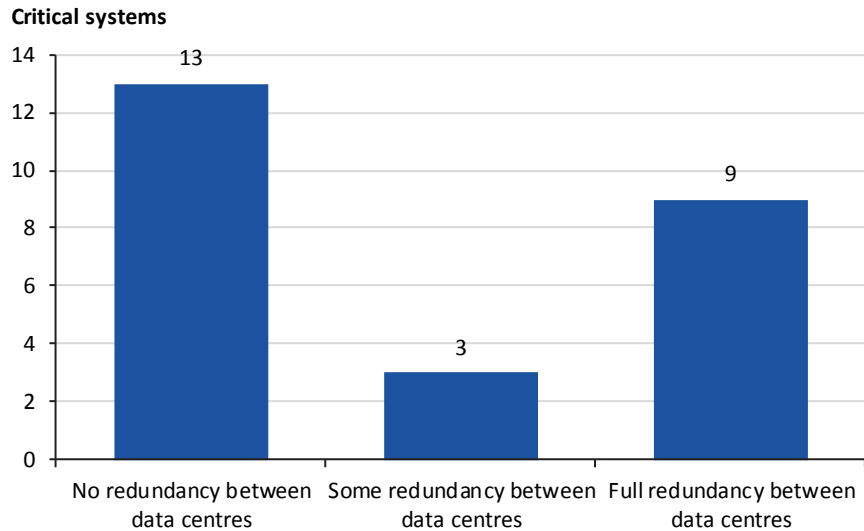
Other audited agencies host most of their systems at purpose-built data centres operated by CenITex, a government body that provides centralised ICT support. In addition, third-party providers host a small number of their systems.

Redundancy of outsourced systems

Agencies need to consider effective redundancy capability to increase their systems' reliability and availability. Six of the seven government departments and their associated agencies outsource the hosting of the majority of their systems to CenITex (the Department of Education and Training hosts and maintains most of its systems in-house).

CenITex submitted a paper to the Victorian Secretaries' Board in November 2016 highlighting the recoverability limitations if one of its data centres was unavailable. Only 36 per cent of the 25 most important systems identified by agencies that are hosted by CenITex have secondary stand by systems to provide a full and rapid recovery of systems, as shown in Figure E.

Figure E
Critical systems hosted at CenITex



Source: VAGO, based on data from CenITex.

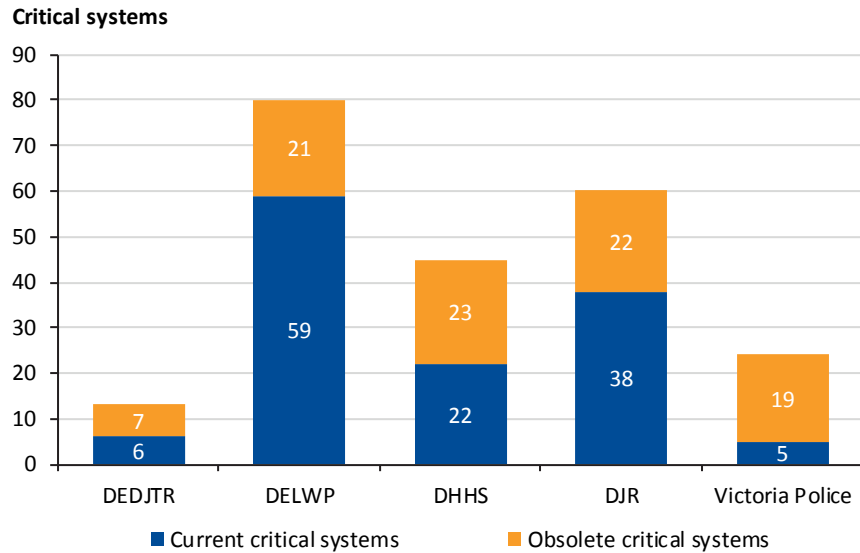
Thirteen of the remaining systems have no redundancy capability—including systems that provide services for criminal justice, marine safety and bushfire management.

Agencies intend to reassess these 25 most important systems, review their order of priority, and identify the estimated investment required to establish and maintain an appropriate level of redundancy. No date has been set for this activity to occur.

Obsolescence in systems

In the audited agencies, 41 per cent of the systems that support critical business functions are obsolete. Figure F shows the number of obsolete systems supporting critical business functions such as financial management, child protection and management of criminal justice, based on information provided by the audited agencies.

Figure F
Obsolete critical systems in the audited agencies



Source: VAGO.

At 79 per cent, Victoria Police has the highest percentage of systems that are obsolete, and DELWP has the lowest at 26 per cent.

The high rate of system obsolescence across all agencies is because:

- agencies do not maintain detailed registers of their systems with enough version information to enable effective monitoring
- agencies only consider and review obsolescence when a system is approaching or is already at the end of its life
- maintaining software and hardware compatibility across a variety of technology platforms is complex and difficult—software components are often heavily customised, which inhibits the upgrade process due to potentially high upgrade costs
- life cycle planning of systems is inadequate and often not performed regularly enough to ensure that systems are refreshed on a regular basis.

All agencies have identified obsolescence in systems as one of the key risks in their enterprise risk register. To manage the risk, agencies are implementing programs to upgrade and replace obsolete systems, although these are not occurring frequently enough and often only when systems are approaching their end of life.

When government agencies run systems that are close to or beyond their end of life, they increase the risk of these systems not being fit for purpose and, consequently, the risk of poor or degraded service delivery. Systems that operate on obsolete hardware or software present a significant disaster recovery risk, because of the limited availability of hardware spare parts, vendor technical support, and staff knowledge and skill. At worst, agencies risk catastrophic equipment failure, extended outage of public services, and exploitation of vulnerable systems by computer virus attacks.

Recommendations

We recommend that the Department of Economic Development, Jobs, Transport and Resources, the Department of Environment, Land, Water and Planning, the Department of Health and Human Services, the Department of Justice and Regulation and Victoria Police:

1. appoint a team of suitably qualified and experienced professionals to form a collaborative disaster recovery working group to:
 - provide advice and technical support
 - share lessons learnt based on disaster recovery tests and exercises
 - coordinate disaster recovery requirements for resources shared between agencies
 - identify, develop, implement and manage initiatives that may impact multiple agencies
 - coordinate funding requests to ensure critical investments and requirements are prioritised
2. perform a gap analysis on their disaster recovery requirements and resource capabilities to determine the extent of the capability investment that will be required
3. develop disaster recovery plans for the systems that support critical business functions and test these plans according to the disaster recovery test program
4. provide advice and training to staff on:
 - newly developed frameworks, policies, standards and procedures to increase awareness and adoption as needed
 - specific disaster recovery systems
5. establish system obsolescence management processes to:
 - identify and manage systems at risk of becoming obsolete, those that will soon have insufficient support or those that will be difficult to manage when they become obsolete
 - enable strategic planning, life-cycle optimisation and the development of long-term business cases for system life-cycle support
 - provide executive with information to allow risk-based investment decisions to be made.

We recommend that the Department of Economic Development, Jobs, Transport and Resources, the Department of Health and Human Services, the Department of Justice and Regulation and Victoria Police:

6. set up disaster recovery frameworks to provide guidelines and minimum standards for ICT disaster recovery planning, including:
 - developing a strategy to establish the minimum levels of readiness and appropriate governance oversight
 - establishing the requirements, frequency and format of disaster recovery tests based on systems' criticality
 - establishing policies, standards and procedures for a consistent approach.

We recommend that the Department of Environment, Land, Water and Planning:

7. update its business impact analysis to identify:
 - system dependencies for critical business functions
 - requirements for the system recovery time objective and recovery point objective
8. determine a recovery strategy for systems that support critical business functions.

We recommend that the Department of Health and Human Services:

9. update its Business Continuity Policy to require business units to consult with system owners and the Business Technology and Information Management group as part of the business impact analysis process, to validate the maximum allowable outage and recovery time objectives
10. update the business impact analysis process to identify system dependencies for critical business functions
11. determine a recovery strategy for systems that support critical business functions.

We recommend that the Department of Justice and Regulation:

12. update its Crisis and Continuity Policy to require business units to consult with system owners and the Knowledge, Information and Technology Services group as part of the business impact analysis process, to validate the maximum allowable outage and recovery time objectives
13. develop a framework to assist business units to determine the criticality of business functions and identify disaster recovery requirements
14. determine a recovery strategy for systems that support critical business functions
15. update the business impact analysis process to include components that:
 - evaluate and rank the criticality of business functions
 - analyse impacts caused by disruption to critical business functions.

Responses to recommendations

We have consulted with DEDJTR, DELWP, DHHS, DJR and Victoria Police, and we considered their views when reaching our audit conclusions. As required by section 16(3) of the *Audit Act 1994*, we gave a draft copy of this report to those agencies and asked for their submissions and comments. We also provided a copy of the report to the Department of Premier and Cabinet.

The following is a summary of those responses. The full responses are included in Appendix A.

All of the audited agencies accepted the recommendations. DEDJTR, DHHS, DJR and Victoria Police provided detailed action plans on how they have begun to address our recommendations and the time frames for these activities. DELWP noted the findings in the report. It outlined its work to assess its ICT assets and systems under its ICT Criticality Framework and will work closely with the other audited agencies to enhance its disaster recovery planning capabilities.

1

Audit context

The Victorian Government delivers a diverse range of services that are important to the economic and social wellbeing of Victorians—from management of state finances to child protection and criminal justice.

The capacity to deliver these services depends in part on the availability and reliability of ICT systems. Being unable to access these systems for an extended period—particularly those used to deliver essential services—could have significant consequences for individuals and for the state, including major cost implications. Disruptions to non-essential services can also result in inconvenience and inefficiencies.

Government agencies face situations within and outside their control that may disrupt their services. These range from equipment failure, fire and theft through to malicious activity and natural disasters.

To respond effectively to major disruptions, including loss of systems, agencies need to design and implement systems and procedures that will support the continuation and resumption of their services.

1.1 ICT disaster recovery

Business continuity management covers the overall process of managing a disruption and re-establishing critical business functions. A key part of any agency's response to a disruption is providing the necessary resources for the agency to continue delivering critical business functions.

ICT disaster recovery is one element of business continuity management—it is the mechanism that agencies use to recover their systems following a major disruption.

Business impact analysis

A BIA is the basis for planning an effective disaster recovery program. It identifies business functions that are critical to the daily operations of an agency. The BIA identifies how much time business functions have to return to full or acceptable degraded level of operation following a disruption.

The Australian and New Zealand standard for managing disruptions—AS/NZS 5050:2010 *Business continuity – Managing disruption-related risk*—states that agencies should perform a BIA as part of an effective risk management program.

An agency's BIA should define its recovery time objective and recovery point objective for restoring systems—see Figure 1A for definitions. The agency's disaster recovery plans should enable it to meet these objectives.

The results of the BIA help the agency to prioritise business functions and allocate resources, as well as informing its investment in recovery strategies.

Key terms

Figure 1A defines the key terms we use in this report.

Figure 1A
Key definitions in ICT disaster recovery

Term	Definition
Business continuity management	The discipline of managing essential business operations and ensuring they continue following a disruption, possibly at a degraded rate or at a level acceptable to key stakeholders.
Business continuity planning	The process of developing a practical plan for how the business can prepare for and continue to operate after a disruption.
Business impact analysis	A management-level analysis that evaluates the risks of disruption to critical business functions, including consideration of the impacts of capability loss over time, and resource needs and their interdependencies.
Critical business function	A function that an agency needs to effectively achieve its objectives.
Data centre	A facility used to house systems and associated components, such as telecommunications, backup power supplies and environmental controls such as air conditioning, fire suppression and security devices.
Disruption	An event that threatens business survival or significantly disrupts normal business operations beyond the business's usual capability for managing operational faults.
Maximum allowable outage	The maximum period of time that an agency can tolerate the disruption of a critical business function, before the achievement of its objectives is adversely affected.
Obsolescence	A state in which systems have become out of date because they are no longer supported by the vendor.
Recovery time objective	The target time required for the recovery of an ICT system after a disruption.
Recovery point objective	The point in time to which an agency must restore data after a disruption—for example, restoring data to the end of the previous day's processing.
Redundancy	The addition of a secondary system to the primary system, to enable continuous system operation in the event that the primary system fails.

Source: VAGO, based on ANAO, *Business Continuity Management*, 2014.

Disaster recovery framework

The Victorian Government Risk Management Framework (VGRMF) sets out the minimum risk management requirements that an agency must meet to demonstrate that it is managing risk effectively, including risks to other agencies and significant risks for the state.

The VGRMF adopts the Australian and New Zealand standard for risk management—AS/NZS ISO 31000:2009 *Risk management – Principles and guidelines*—which provides a generic, internationally accepted standard for best practice risk management.

The standard encourages agencies to establish an effective framework for managing risk, setting the agency's policy, demonstrating commitment, providing resources, assigning responsibilities and monitoring progress.

An effective framework for disaster recovery consists of an overarching disaster recovery policy and relevant standards and guidelines covering:

- governance and strategy for disaster recovery
- disaster recovery processes and controls
- creation, testing and maintenance of disaster recovery plans
- awareness and training on disaster recovery.

Disaster recovery plans

According to AS/NZS 5050:2010, having a disaster recovery plan improves an agency's ability to respond quickly and effectively to a disruption. As agencies become more reliant on ICT systems to run their operations, the importance of disaster recovery planning for the recovery of these systems increases.

Disaster recovery testing

Disaster recovery testing helps agencies verify their ability to recover ICT systems after a disruption. A disaster recovery test involves recovering and restoring a system by following the procedures defined in a disaster recovery plan. AS/NZS 5050:2010 states that agencies should conduct periodic disaster recovery tests to ensure that disaster recovery plans will work effectively.

Disaster recovery training

The international standard ISO/IEC 27031:2011 *Guidelines for information and communication technology readiness for business continuity* states: 'A co-ordinated program should be implemented to ensure that processes are in place to regularly promote disaster recovery awareness in general, as well as assess and enhance competency of all relevant personnel key to the successful implementation of disaster recovery.'

Training is an important component of an effective disaster recovery framework—it helps staff gain knowledge and skills to manage the recovery of a system following a disruption. Active participation in disaster recovery tests and theoretical training are key methods for developing staff skills and competencies.

Outsourcing disaster recovery services

Government agencies can outsource the hosting and disaster recovery of ICT systems to third-party service providers, although outsourcing does not absolve agencies of all responsibilities for disaster recovery. There must still be careful planning and integration between the agency and the service provider.

CenITex is an ICT shared services agency set up by the Victorian Government in 2008 to centralise ICT support for government departments and agencies. CenITex delivers ICT infrastructure, application hosting and desktop services.

CenITex provides ICT services to six of the seven Victorian Government departments and their associated agencies (rather than use CenITex's services, the Department of Education and Training hosts and maintains most of its systems in-house). CenITex also provides agencies with optional disaster recovery services. CenITex and agencies establish memorandums of understanding to define their roles, responsibilities and requirements.

Contracts with third-party service providers and memorandums of understanding with CenITex set out terms of service and parties' responsibilities. By establishing responsibilities and requirements, third-party service providers and government agencies can monitor and report on how they are managing service delivery, including disaster recovery.

Recovery of systems and services hosted by CenITex

In 2016, CenITex developed a framework that provides a recovery order for systems that it hosts, in the event of a data centre loss. This framework was developed in consultation with all seven Victorian portfolio departments and the Department of Premier and Cabinet's Emergency Management and Enterprise Solutions branches. The departments have agreed to a combined recovery order for 25 of their most important systems.

In November 2016, CenITex submitted a paper to the Victorian Secretaries' Board outlining the key recoverability limitations for these systems if one of CenITex's data centres became unavailable:

- Core systems—such as network, email, desktop, security and support services—would take significant time to restore and would only be restored to a reduced capacity.
- Some of the 25 most important systems do not have redundancy capability. A secondary stand-by system would enable full and rapid recovery of the system.

CenITex plans to improve its business services, reduce the impact of system outages and improve the recoverability of these systems. The departments plan to review the priority order of their 25 most important systems and estimate the investment required to establish and maintain their recoverability.

1.2 ICT asset management

A better practice approach to ICT asset management involves acquiring, using and disposing of ICT assets to maximise service delivery over an asset's useful life. Life cycle management mitigates risk and helps define and plan the cost of updating and replacing assets when they become obsolete.

Asset management policy and guidance

The Department of Treasury and Finance (DTF) provides guidance to Victorian Government agencies to help them develop and implement good asset management practices. DTF administers a range of financial management policies and frameworks, including the Victorian Government Asset Management Accountability Framework (AMAF), published in February 2016. The AMAF establishes a set of mandatory requirements and general guidance for government agencies to manage their assets, including ICT assets.

Figure 1B shows the key elements of the AMAF that government agencies should consider in managing assets throughout their life cycle.

Due to the shorter life cycle of ICT assets, some elements of the model may need to be concurrent, with planning for the next generation of ICT assets often needing to begin as soon as a new ICT asset is implemented.

Figure 1B
The AMAF asset life cycle



Source: DTF.

Managing obsolescence in systems

Under the *Financial Management Act 1994*, agencies and their accountable officers are responsible for identifying and managing their assets, including ICT assets. This includes developing and implementing risk-management strategies.

To manage risk, an agency must identify, assess and prioritise existing and potential risks, enabling it to mitigate and manage potential impacts by implementing new policies and procedures.

There are a number of risks associated with ageing and obsolescence that are common to all assets. These risks are particularly acute for ICT assets due to the high speed of innovation in ICT. Unlike other assets with relatively long life spans, ICT assets can quickly become obsolete if not managed carefully.

Inadequate management of obsolescence in ICT systems can lead to poor or degraded service delivery by government agencies. At worst, it could lead to catastrophic equipment failure, extended outage of a public service, or exploitation of vulnerable systems by computer virus attacks.

1.3 Legislation and standards

Standing Directions of the Minister for Finance 2016

The Standing Directions of the Minister for Finance 2016, which supplement the *Financial Management Act 1994*, require agencies to develop, implement and maintain documented business continuity planning processes consistent with the latest Australian, New Zealand, international or industry-recognised standard.

Victorian Protective Data Security Framework and Standards

The Victorian Protective Data Security Framework (VPDSF) and the Victorian Protective Data Security Standards (VPDSS) establish mandatory requirements to protect public sector data and provide for governance across the four domains of information, personnel, ICT and physical security. Under the VPDSS, agencies must have effective business continuity processes in place to enable them to respond to and recover from any event that affects the confidentiality, integrity and availability of public sector data.

Government departments and Victoria Police must comply with the VPDSF and VPDSS requirements by July 2018. Previously, Victoria Police had to comply with the Standards for Law Enforcement Data Security, but it now operates under the VPDSS.

Practice standards

The following standards include relevant principles for better practice disaster recovery processes and controls:

- ISO 22301:2012 *Societal security – Business continuity management systems – Requirements*
- AS/NZS 5050:2010 *Business continuity – Managing disruption-related risk*
- ISO/IEC 27031:2011 *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity.*

Other better practice standards relevant to maintaining effective disaster recovery processes and controls include:

- *Business continuity management: Building resilience in public sector entities* (better practice guide), Australian National Audit Office, June 2009
- *Contingency Planning Guide for Federal Information Systems* (NIST Special Publication 800-34 Rev. 1), National Institute of Standards and Technology (United States), May 2010.

The following standards include relevant principles for process assessment as a basis for use in determining process capability:

- ISO/IEC 15504-2:2003 *Information technology – Process assessment*
- *COBIT Process Assessment Model: Using COBIT 5*, 2013—see Appendix B for descriptions of the capability ratings.

1.4 Why this audit is important

The use of ICT systems has fundamentally changed how agencies operate. Agencies depend on systems to:

- deliver public services—including essential services—to the Victorian community
- efficiently and effectively manage government operations
- fulfil their statutory obligations.

Agencies need to have effective processes to recover systems in the event of a disruption. As ICT systems become increasingly critical for government operations and the wider Victorian community, the need to ensure systems can continue to operate and be recovered rapidly in the event of a disruption is growing.

1.5 Previous audits

Our audits have consistently found weaknesses in both business continuity planning and ICT disaster recovery planning.

Our November 2013 report *Portfolio Departments and Associated Entities: Results of the 2012–13 Audits* included results of our assessment of departments' business continuity and disaster recovery processes. We identified limited awareness and management of disaster recovery capabilities and processes which resulted in risks for departments' and agencies' ability to recover operations and provide essential public services in the event of a disruption.

Our October 2014 report *Information and Communications Technology Controls Report 2013–14* reported similar weaknesses in agencies' ICT disaster recovery processes and controls. We identified these findings again in our October 2015 report *Financial Systems Controls Report: Information Technology 2014–15*.

1.6 What this audit examined and how

Our objective was to determine whether selected departments and Victoria Police can effectively recover their critical ICT systems and data in the event of a disruption.

We assessed whether these agencies had plans and processes in place for:

- identifying critical information assets and infrastructure, and prioritising their recovery through a BIA
- recovering critical information assets and infrastructure that support critical business functions as identified by the BIA
- periodically testing critical information assets and infrastructure that support critical business functions to validate their disaster recovery capability
- using data centres to host systems and provide redundancy capabilities
- ensuring contracts for outsourced disaster recovery services are robust
- conducting a maintenance program to identify, manage and upgrade obsolete systems
- ensuring continuous improvement in monitoring, evaluating and reporting on agencies' level of preparedness for disaster recovery.

Taking a risk-based approach, we focused on Victoria Police and four departments that rely heavily on systems to provide critical government services. The audited agencies are DEDJTR, DELWP, DHHS, DJR and Victoria Police.

We conducted this audit in accordance with section 15 of the *Audit Act 1994* and Australian Auditing and Assurance Standards. The total cost of this audit was \$455 000.

In accordance with section 20(3) of the *Audit Act 1994*, we express no adverse comment or opinion about anyone we name in this report.

1.7 Report structure

The remainder of this report is structured as follows:

- Part 2 discusses the results of our assessment for DEDJTR
- Part 3 discusses the results of our assessment for DELWP
- Part 4 discusses the results of our assessment for DHHS
- Part 5 discusses the results of our assessment for DJR
- Part 6 discusses the results of our assessment for Victoria Police.

2

Department of Economic Development, Jobs, Transport and Resources

In this part of the report, we assess whether DEDJTR can effectively recover its critical ICT systems and data if a disruption occurs.

DEDJTR's disaster recovery processes are not robust enough to effectively and efficiently recover all critical systems after a disruption. DEDJTR currently only has capability to recover selected critical systems. The department needs to further develop its disaster recovery processes and capabilities to minimise any loss of critical services in the event of a disruption.


2.1 Business impact analysis

DEDJTR's Technology Services division is responsible for implementing disaster recovery requirements for ICT systems that it supports. Business groups own and manage the systems and are responsible for managing their recovery if a disruption occurs.

Figure 2A summarises our assessment of DEDJTR's BIA process and its components against COBIT 5 ISO/IEC 15504-based capability levels and a maturity rating system based on the ISO/IEC 15504-2:2003 standard—see Appendix B for descriptions of the capability ratings.

Figure 2A

Assessment of DEDJTR's BIA process and components

BIA process—overall capability 	
Component	Capability rating
List all of the critical business processes that underpin achievement of the agency's objectives	Partially achieved
Rank the processes in order of importance to the agency's objectives and exclude those processes not considered critical to achieving the objectives	Partially achieved
Consider process interdependencies that exist	Partially achieved
Determine the minimum requirements necessary to perform each critical process	Partially achieved
Obtain executive endorsement of prioritised list of critical business processes	Partially achieved
Evaluate the impacts of a loss of each critical process according to the agency's objectives	Partially achieved
Identify interim processing procedures (alternative or manual processing) or techniques to be adopted during the recovery phase	Partially achieved
Determine the maximum allowable outage for each critical process	Partially achieved
Determine internal and external critical interdependencies	Partially achieved
Identify vital records	Partially achieved
Determine the recovery time objective for each critical business process and ICT system	Partially achieved
Determine the recovery point objective for data	Partially achieved
Obtain executive endorsement of the BIA	Partially achieved

Source: VAGO.

DEDJTR's former arrangements for significant business disruptions were an aggregation of business continuity plans and processes prepared for predecessor departments. These varied in approach and format. DEDJTR has developed a new business continuity management policy and framework, which it is currently implementing and expects to complete by 30 November 2017. The new business continuity management policy and framework includes the implementation of a department-wide BIA that will identify the processes, systems and resources required to recover its essential business functions.

Once completed, the business continuity management framework and BIA should:

- ensure that the Technology Services and Emergency Management divisions are consulted on the identification of systems and dependencies
- ensure that business areas consult with Technology Services to identify realistic recovery time and recovery point objectives for their systems
- provide information to Technology Services about systems, maximum acceptable outages and recovery time objectives identified in business continuity plans.

DEDJTR's intended approach is reasonable and aligns with better practice standards. As DEDJTR is currently implementing this process, it was only able to provide limited evidence to demonstrate that it will achieve the above.


Until DEDJTR implements its new policy and framework, it will continue to use 2014 business continuity requirements for systems identified as needing disaster recovery capability.

Once DEDJTR has implemented the BIA, it plans to conduct the analysis every two years unless significant changes in the department's structure or strategic direction trigger an earlier review.

2.2 Disaster recovery

Figure 2B summarises our assessment of DEDJTR's disaster recovery framework and its components against COBIT 5 ISO/IEC 15504-based capability levels and ISO/IEC 15504-2:2003 respectively.

Figure 2B
Assessment of DEDJTR's disaster recovery process and components

Disaster recovery process—overall capability 	
Component	Capability rating
Maintain an ICT disaster recovery continuity framework	Partially achieved
Review, maintain and improve the ICT disaster recovery plans	Partially achieved
Conduct ICT disaster recovery plan testing	Achieved
Conduct ICT disaster recovery training	Not achieved

Source: VAGO.

The implementation of disaster recovery capabilities for ICT systems depends on business requirements identified through the BIA. The BIA resulting from DEDJTR's business continuity management refresh program—expected to be completed by 30 November 2017—should verify whether there are additional systems that need disaster recovery capability.

DEDJTR is reviewing the current process. In its current form, the process does not effectively ensure a standardised department-wide approach for planning, implementing and managing disaster recovery requirements to support DEDJTR's essential business functions.

The Technology Services division is now developing the necessary governance arrangements, frameworks and policies to better manage a comprehensive and prioritised approach to disaster recovery and expects to complete this process by 31 January 2018. Once completed, it should:

- coordinate the development and maintenance of disaster recovery plans with the relevant service providers
- coordinate the testing of critical systems with relevant service providers.

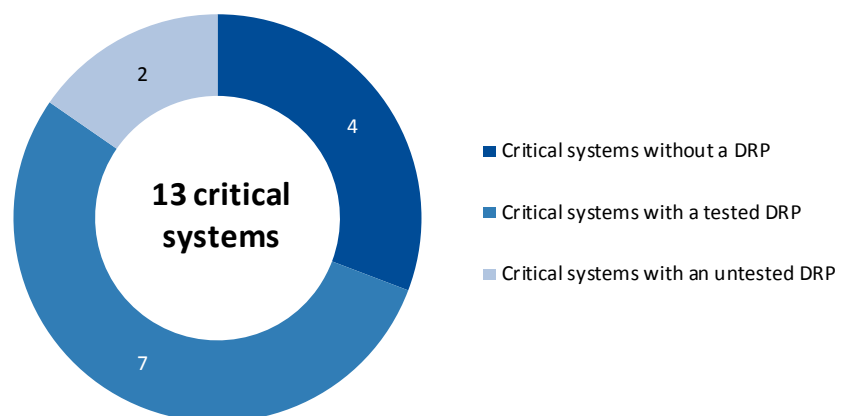
DEDJTR's intended approach aligns with better practice standards.

Disaster recovery plans and testing

Since the formation of the department in 2015, DEDJTR has not identified all of the systems that support its critical business functions or determined a recovery strategy for each system, including whether the system requires disaster recovery capability.

Disaster recovery plans exist for nine of DEDJTR's 13 systems that support critical business functions. Seven of these nine systems have a tested disaster recovery plan, as shown in Figure 2C.

Figure 2C
DEDJTR's critical systems and disaster recovery plans



Note: DRP = disaster recovery plan.

Source: VAGO, based on information from DEDJTR.

Individual business groups and Technology Services perform functional disaster recovery tests on seven of these systems annually. Since 1 January 2015, DEDJTR has commissioned an annual independent service assurance review of the ICT control environment for three of these systems—which includes a component of disaster recovery.

Functional disaster recovery tests verify DEDJTR's ability to recover systems based on business recovery requirements previously identified by the former Department of State Development, Business and Innovation and the former Department of Transport, Planning and Local Infrastructure. DEDJTR has not validated these business recovery requirements.

Disaster recovery training

DEDJTR performs functional disaster recovery tests on its critical systems but does not provide theoretical awareness training to staff with specific disaster recovery roles and responsibilities.

Once DEDJTR's Technology Services division has developed the disaster recovery governance arrangements, frameworks and policies, it intends to:

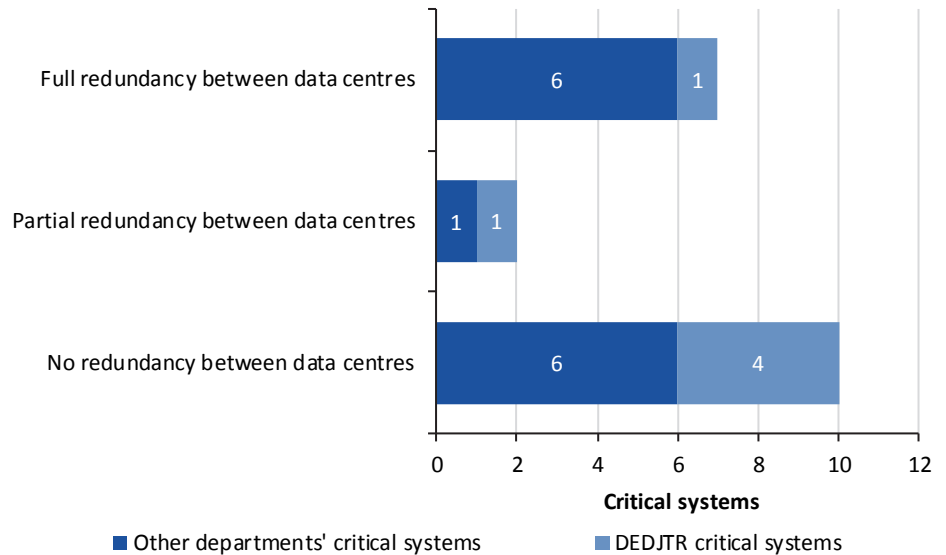
- inform relevant departmental business groups so they can plan, implement and manage disaster recovery of their systems
- provide training for staff on their roles and responsibilities in a disaster recovery event, to prepare them for participation in exercises, tests and actual emergency situations
- conduct a post-test review to evaluate the disaster recovery response process, to identify and correct any weaknesses, to determine strengths and to promote continuous improvements in the disaster recovery process.

Outsourced disaster recovery arrangement with CenITex

DEDJTR engages CenITex for specific disaster recovery services, including annual disaster recovery testing and hosting disaster recovery capability of selected systems at the CenITex data centre. CenITex and DEDJTR manage the terms and conditions of these specific disaster recovery services through statement-of-work documents.

Figure 2D shows the extent of redundancy capability in DEDJTR's and the other audited agencies' critical systems hosted by CenITex.

Figure 2D
Redundancy capability in DEDJTR's and other agencies' critical systems hosted by CenITex



Note: Nineteen of the 25 critical systems hosted by CenITex belong to the in-scope audited agencies.

Source: VAGO, based on data from CenITex.

Not all of DEDJTR's critical systems hosted by CenITex have redundancy capabilities. DEDJTR's business continuity management framework review should produce a new department-wide BIA and verify whether:

- the four systems hosted by CenITex that do not currently have redundancy capabilities need such capability
- the business requirements to have redundancy capabilities—partial or full—for the two systems hosted by CenITex are still valid.

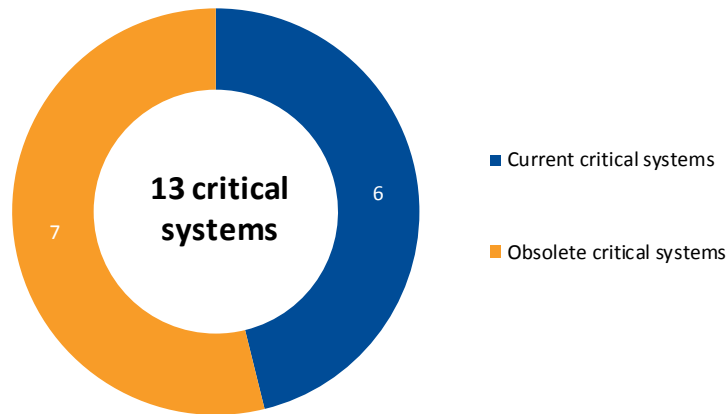
2.3 Obsolescence in systems

DEDJTR's business groups are responsible for managing their own systems' life cycles. They can consult with Technology Services for advice on managing system obsolescence.

DEDJTR also relies on CenITex for managing infrastructure equipment and has supplemented its infrastructure expenditure with specific funding initiatives when required.

Figure 2E shows the number of systems supporting critical business functions at DEDJTR that it reports as being obsolete.

Figure 2E
Obsolete critical systems at DEDJTR



Source: VAGO.

DEDJTR identifies and tracks system obsolescence for corporate systems through its enterprise risk management process. DEDJTR upgrades or replaces these systems based on business case submissions.

DEDJTR's business groups are responsible for their own business systems, and must identify their requirements, obtain funding and liaise with Technology Services to assist with mobilising replacement projects.

This process is not effective for centrally identifying and managing the risk of system obsolescence. DEDJTR's business groups need to take greater responsibility for actively managing obsolescence in their systems. They need to use the business continuity management process as it matures to obtain system life cycle information to help them better identify and manage system obsolescence.

3

Department of Environment, Land, Water and Planning

In this part of the report, we assess whether DELWP can effectively recover its critical ICT systems and data if a disruption occurs.

DELWP's disaster recovery processes are not robust enough to effectively and efficiently recover all critical systems after a disruption. DELWP currently only has capability to recover selected critical systems. The department needs to further develop its disaster recovery processes and capabilities to minimise any loss of critical services in the event of a disruption.

3.1 Business impact analysis

Divisions within DELWP manage their own disaster recovery requirements and capabilities, and manage business continuity with support from the Business Governance Services branch. DELWP has developed a business continuity and resilience management framework to set business continuity guidelines and a disaster recovery framework to set disaster recovery planning guidelines for the divisions.


DELWP's Business Governance Services branch coordinates with the department's divisions to perform, review and update their BIAs annually as part of business continuity. Each BIA identifies the division's critical business functions, resource requirements and any supporting system that may require disaster recovery capability.

DELWP formalised its business continuity policies and procedure documents in 2015.

Figure 3A summarises our assessment of DELWP's BIA process and its components against COBIT 5 ISO/IEC 15504-based capability levels and a rating system based on the ISO/IEC 15504-2:2003 standard—see Appendix B for descriptions of the capability ratings.

Figure 3A

Assessment of DELWP's BIA process and components

BIA process—overall capability 	
Component	Capability rating
List all of the critical business processes that underpin achievement of the agency's objectives	Largely achieved
Rank the processes in order of importance to the entity's objectives and exclude those processes not considered critical to achieving the objectives	Partially achieved
Consider process interdependencies that exist	Largely achieved
Determine the minimum requirements necessary to perform each critical process	Largely achieved
Obtain executive endorsement of prioritised list of critical business processes	Largely achieved
Evaluate the impacts of a loss of each critical process according to the agency's objectives	Largely achieved
Identify interim processing procedures (alternative or manual processing) or techniques to be adopted during the recovery phase	Largely achieved
Determine the maximum allowable outage for each critical process	Largely achieved
Determine internal and external critical interdependencies	Partially achieved
Identify vital records	Partially achieved
Determine the recovery time objective for each critical business process and ICT system	Not achieved
Determine the recovery point objective for data	Partially achieved
Obtain executive endorsement of the BIA	Largely achieved

Source: VAGO.

DELWP's BIA process identifies time-critical business functions and their various dependencies, including systems, human resources, third-party service providers, utilities and infrastructure. The BIA process focuses on identifying contingencies for the recovery of critical business functions within the functions' maximum allowable outage time.

DELWP divisions are not consistently identifying systems' dependencies or the recovery time objective and recovery point objective as part of the BIA process. These information gaps may affect how DELWP determines a critical business function's maximum allowable outage time, as DELWP may need to recover specific systems first to enable the effective recovery of critical business functions.

DELWP advised that it plans to collect and assess this information in future annual review cycles as the process matures.


3.2 Disaster recovery

In July 2015, DELWP's internal audit reported weaknesses in its disaster recovery processes. The report found that:

- DELWP did not have a coordinated department-wide approach to disaster recovery planning
- disaster recovery policies and procedure documents had been drafted but not yet formalised
- identification and criticality assessment of systems had not been recently performed and there was no clear alignment of ICT disaster recovery plans with business requirements.

Figure 3B summarises our assessment of DELWP's disaster recovery process and its components against COBIT 5 ISO/IEC 15504-based capability levels and ISO/IEC 15504-2:2003 respectively.

Figure 3B
Assessment of DELWP's disaster recovery process and components

Disaster recovery process—overall capability 	
Component	Capability rating
Maintain an ICT disaster recovery continuity framework	Partially achieved
Review, maintain and improve the ICT disaster recovery plans	Partially achieved
Conduct ICT disaster recovery plan testing	Partially achieved
Conduct ICT disaster recovery training	Not achieved

Source: VAGO.

At the time of the July 2015 internal audit, DELWP developed a new ICT operating model to introduce clear accountability, responsibility and consistency for managing and delivering ICT services. Since the audit, DELWP has developed policies, procedures and guidance documents to coordinate and support ICT disaster recovery planning.

DELWP's business divisions are accountable for funding, resourcing and making decisions about the ICT services that support business processes. DELWP is gradually adopting the policies and procedures that it has developed as part its ICT disaster recovery planning process.

DELWP also developed a criticality framework—a set of policies, procedures and tools to identify and support management of critical ICT systems under the new ICT operating model. The criticality framework states that DELWP divisions will be responsible for assessing their systems to determine if they are critical. The divisions responsible for managing critical systems will be required to complete annual assessments of the systems—including managing disaster recovery.

DELWP reported that it expects the maturity of disaster recovery processes to improve over time as it implements the ICT operating model and criticality framework, enabling it to monitor the overall condition of its ICT systems.

DELWP will need to maintain a coordinated department-wide approach to disaster recovery by ensuring that divisions receive guidance on their approach and adhere to the new criticality framework.

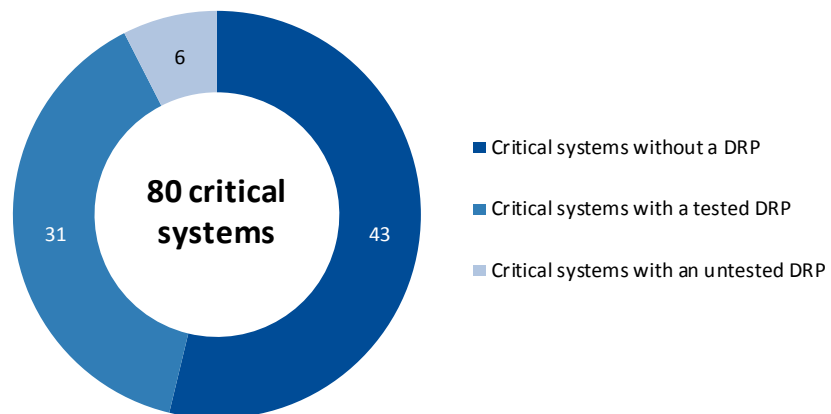
Disaster recovery plans and testing

DELWP has disaster recovery plans for 37 out of 80 systems that divisions manage independently. There is no consistent department-wide approach for functional disaster recovery tests, because individual divisions determine the type and timing of tests they perform. The divisions do not have a testing schedule that determines the priority, frequency and scope of testing disaster recovery plans.

Functional recovery tests performed by DELWP verify whether it can recover the system, but not whether this can occur in line with business recovery requirements—because DELWP has not determined them.

Figure 3C shows the number of systems supporting critical business functions at DELWP that have a disaster recovery plan.

Figure 3C
DELWP's critical systems and disaster recovery plans



Note: DRP = disaster recovery plan.

Source: VAGO, based on information from DELWP.

DELWP has not tested the recoverability of the remaining 43 systems supporting critical business functions. There are no disaster recovery plans for these systems, and it is unclear whether these systems require disaster recovery capability.

DELWP advised that it expects the oversight and management of testing critical systems with disaster recovery capability to improve over time as it implements the new ICT operating model and criticality framework. Until the oversight of these systems improves, DELWP leaves itself at risk of being unable to support critical business functions during a disruption and extended outage of systems.

Disaster recovery training

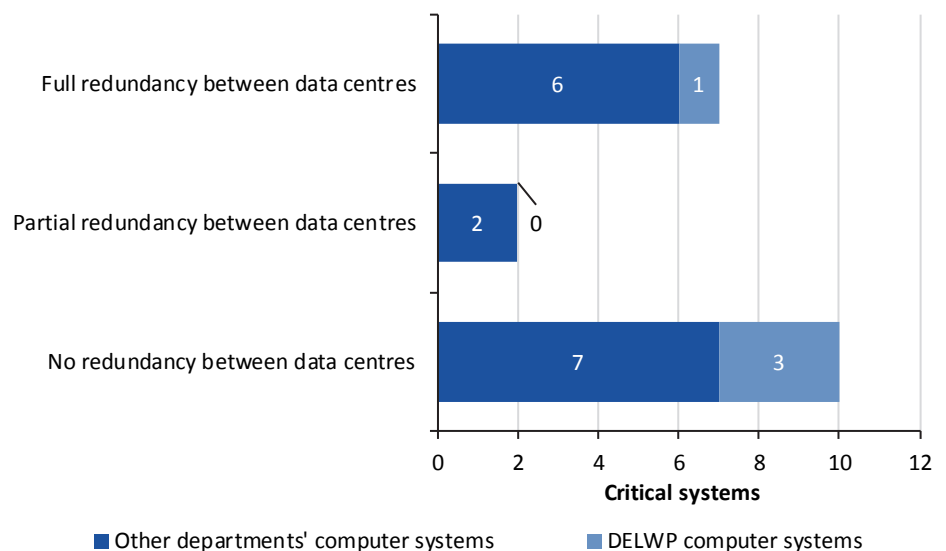
DELWP performs functional disaster recovery tests on its critical systems but does not provide theoretical awareness training to staff with specific disaster recovery roles and responsibilities.

Outsourced disaster recovery arrangement with CenITex

DELWP engages CenITex for specific disaster recovery services, including annual disaster recovery testing and hosting disaster recovery capability of selected systems at the CenITex data centre. CenITex and DELWP manage the terms and conditions of these specific disaster recovery services through statement-of-work documents.

Figure 3D shows the extent of redundancy capability in DELWP's and the other audited agencies' critical systems hosted by CenITex.

Figure 3D
Redundancy capability in DELWP's and other agencies' critical systems hosted by CenITex



Note: Nineteen of the 25 critical systems hosted by CenITex belong to the in-scope audited agencies.

Source: VAGO, based on data from CenITex.

DELWP has not performed a criticality assessment of systems to determine whether:

- the three systems hosted by CenITex that do not currently have redundancy capabilities require such capability
- the business requirements to have redundancy capabilities for one system hosted by CenITex are still valid.

In the absence of this assessment, DELWP is unable to determine if its resourcing and funding for the four critical systems hosted at CenITex is appropriate and whether the highest-priority systems have adequate recovery capability in the event of a disaster.

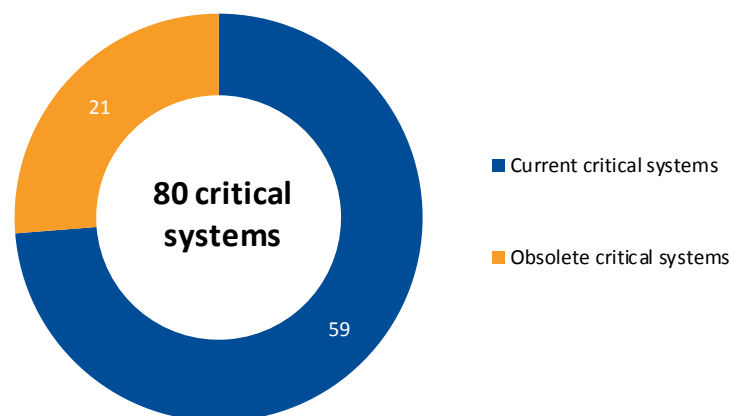
DELWP also needs to determine whether any of its other systems that support critical business functions should require redundancy capabilities.

3.3 Obsolescence in systems

DELWP has begun to identify and assess the health and life cycle stages of its systems. DELWP has developed a system upgrade roadmap consisting of approved and proposed projects up until December 2018. It is identifying initiatives that will deliver new and enhanced ICT services to support its key business functions.

Figure 3E shows the number of systems supporting critical business functions at DELWP that it reports as being obsolete.

Figure 3E
Obsolete critical systems at DELWP



Source: VAGO, based on information from DELWP.

To further manage system obsolescence, divisions will be required to complete an annual system life cycle verification under DELWP's criticality framework, which is in the early stages of implementation. The framework will require divisions to manage the life cycle of systems that support critical business functions, including identifying and managing systems that are obsolete or approaching end of life.

DELWP's ICT Governance Committee has approved the refresh of the department's ICT strategy, beginning in the second quarter of 2017–18, which will provide direction and guidance to divisions about investing in and managing their ICT services.

4

Department of Health and Human Services

In this part of the report, we assess whether DHHS can effectively recover its critical ICT systems and data if a disruption occurs.


DHHS's disaster recovery processes are not robust enough to effectively and efficiently recover all critical systems after a disruption. DHHS currently only has capability to recover selected critical systems. The department needs to further develop its disaster recovery processes and capabilities to minimise any loss of critical services in the event of a disruption.

4.1 Business impact analysis

DHHS is a large department and has about 1 300 users of its systems across 11 divisions. Within DHHS, business units and the Emergency Management branch jointly develop BIAs based on DHHS's business continuity management policy and framework.

Figure 4A summarises our assessment of DHHS's BIA process and its components against COBIT 5 ISO/IEC 15504-based capability levels and a rating system based on the ISO/IEC 15504-2:2003 standard—see Appendix B for descriptions of the capability ratings.

Figure 4A
Assessment of DHHS's BIA process and components

BIA process—overall capability 	
Component	Capability rating
List all of the critical business processes that underpin achievement of the agency's objectives	Largely achieved
Rank the processes in order of importance to the entity's objectives and exclude those processes not considered critical to achieving the objectives	Partially achieved
Consider process interdependencies that exist	Partially achieved
Determine the minimum requirements necessary to perform each critical process	Largely achieved
Obtain executive endorsement of prioritised list of critical business processes	Largely achieved
Evaluate the impacts of a loss of each critical process according to the agency's objectives	Largely achieved
Identify interim processing procedures (alternative or manual processing) or techniques to be adopted during the recovery phase	Largely achieved
Determine the maximum allowable outage for each critical process	Partially achieved
Determine internal and external critical interdependencies	Partially achieved
Identify vital records	Partially achieved
Determine the recovery time objective for each critical business process and ICT system	Not achieved
Determine the recovery point objective for data	Not achieved
Obtain executive endorsement of the BIA	Partially achieved

Source: VAGO.

The business continuity management framework requires DHHS to perform a BIA twice per year or more often when there is a major departmental change. The BIA identifies DHHS's time-critical business functions, resource requirements and dependencies for its ICT systems, equipment and human resources. The BIA also outlines contingency strategies for the recovery of business functions following a disruption.

DHHS's BIA process:

- identifies business functions' maximum allowable outage times, but business units do not always consult with the Business Technology and Information Management branch to validate whether the systems they rely on for business functions can be recovered within the maximum allowable outage time
- does not consistently identify resource dependencies required to recover business functions such as dependencies on systems outside the department
- does not consistently identify the recovery time objective and recovery point objective of systems that support business functions.

Inconsistent identification and evaluation of disaster recovery requirements and system recovery capabilities between business units and Business Technology and Information Management branch will affect DHHS's ability to recover critical business functions in the time required by business units.

4.2 Disaster recovery

In the past, DHHS has relied on business units to determine disaster recovery requirements for their systems, to inform risk-based investment decisions. As a result, DHHS has no central oversight of this process and has been unable to effectively manage disaster recovery for systems that support critical business functions.

In 2016, the Business Technology and Information Management branch began to identify and assess disaster recovery requirements for 20 systems that support business functions. The branch advised that it will perform a gap analysis of the 20 systems' disaster recovery capability and requirements. The branch has commenced this activity and expects to complete it by 30 June 2018.

DHHS established the Disaster Recovery and Business Continuity Planning Reference Group in July 2017 to improve decision-making processes for disaster recovery investment. The group aims to:


- develop an evaluation process to objectively assess risks and compare disaster recovery requirements for competing divisions and systems
- use the newly developed evaluation process to make better risk-based decisions and investments
- provide independent advice to DHHS on the implementation of its disaster recovery strategy.

The reference group will also:

- oversee DHHS's ICT disaster recovery strategy to provide consistent guidance
- ensure policies and standards are in place to support DHHS's recovery objectives and ensure compliance
- work to reduce the confusion in DHHS about the distinct but related topics of business continuity and disaster recovery
- advise on ways of determining requirements, expectations and planning for business continuity and disaster recovery.

Figure 4B summarises our assessment of DHHS’s disaster recovery process and its components against COBIT 5 ISO/IEC 15504-based capability levels and ISO/IEC 15504–2:2003 respectively.

Figure 4B
Assessment of DHHS’s disaster recovery process and components

Disaster recovery process—overall capability	
	
Component	Capability rating
Maintain an ICT disaster recovery continuity framework	Partially achieved
Review, maintain and improve the ICT disaster recovery plans	Partially achieved
Conduct ICT disaster recovery plan testing	Partially achieved
Conduct ICT disaster recovery training	Not achieved

Source: VAGO.

DHHS’s disaster recovery processes are limited, and there is no strategy or framework to manage ICT disaster recovery. The Disaster Recovery and Business Continuity Planning Reference Group has been set up to address these issues. Its objective is to align the two planning processes to ensure a well-managed and coordinated approach to disaster recovery requirements. DHHS has approved additional funding to develop and implement a disaster recovery strategy.

Disaster recovery plans and testing

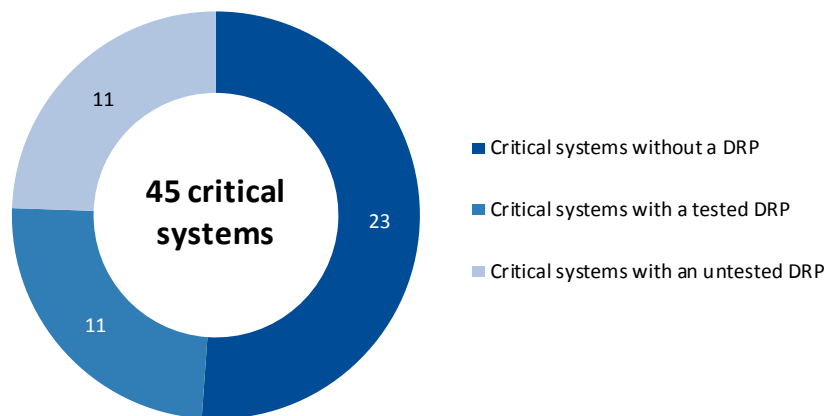
DHHS does not have disaster recovery plans for all of its systems that support critical business functions. Disaster recovery plans currently exist for 11 systems managed by the Business Technology and Information Management branch and previously identified as requiring disaster recovery capability.

The branch performs annual functional disaster recovery tests on these systems. Functional recovery tests verify that DHHS can recover the system, but these tests do not verify whether this can occur in line with business recovery requirements—because DHHS has not determined them.

DHHS has invested in enhancing the disaster recovery capabilities of a number of its critical systems in recent years. DHHS expects other systems’ disaster recovery capabilities will also mature as it implements planned investments in disaster recovery. DHHS plans to allocate the available funds for disaster recovery activities based on risk identification and prioritisation.

Figure 4C shows the number of systems supporting DHHS's critical business functions that have a disaster recovery plan.

Figure 4C
DHHS's critical systems and disaster recovery plans



Note: DRP = disaster recovery plan.

Source: VAGO, based on information from DHHS.

Disaster recovery training

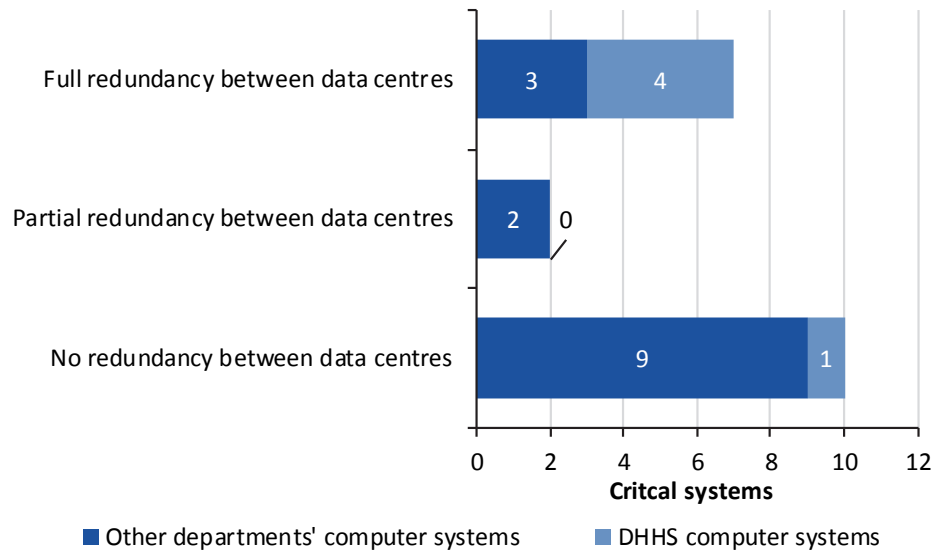
DHHS performs functional disaster recovery tests on its critical systems, but it does not provide theoretical awareness training for staff who have specific roles and responsibilities for disaster recovery.

Outsourced disaster recovery arrangement with CenITex

DHHS engages CenITex for specific disaster recovery services, including annual disaster recovery testing and hosting disaster recovery capability of selected systems at the CenITex data centre. CenITex and DHHS manage the terms and conditions of these specific disaster recovery services through statement-of-work documents.

Figure 4D shows the extent of redundancy capability in DHHS's and the other audited agencies' critical systems hosted by CenITex.

Figure 4D
Redundancy capability in DHHS's and other agencies' critical systems hosted by CenITex



Note: Nineteen of the 25 critical systems hosted by CenITex belong to the in-scope audited agencies.

Source: VAGO, based on data from CenITex.

DHHS is currently replacing the one system that does not have disaster recovery capability. DHHS advised that the new version of this system will incorporate redundancy capability, and it plans to implement it by 30 June 2018.

Disaster recovery compliance

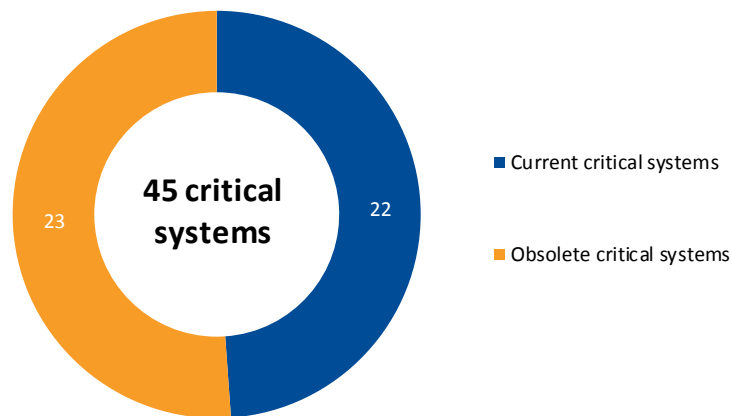
We reviewed DHHS's processes for managing disaster recovery compliance. DHHS does not have a compliance framework, and its processes are not robust enough for it to effectively monitor, measure, evaluate and report compliance on disaster recovery processes. DHHS performs compliance activities for specific systems only.

DHHS has not actively performed audits on its disaster recovery program and processes in the past five years. DHHS needs to conduct regular audits on these elements, as well as annual functional disaster recovery tests.

4.3 Obsolescence in systems

Figure 4E shows the number of systems supporting critical business functions at DHHS that it reports as being obsolete.

Figure 4E
Obsolete critical systems at DHHS



Source: VAGO, based on information from DHHS.

DHHS's executive board evaluates and endorses the annual ICT investment program. Following a period of under-investment, DHHS has begun to fund investments in infrastructure and systems in the past four years.

DHHS has substantial work ahead of it, to develop a mature life cycle management approach for maintaining its critical systems and gaining assurance that those systems remain reliable and are recoverable after a disaster.

DHHS has identified obsolete systems and allocated funds to upgrade these systems—including two of its most critical systems. DHHS is consolidating and documenting information on obsolete systems in its Meta ICT Information Asset and Applications Register to better inform future asset identification and decision-making on system upgrades.

5

Department of Justice and Regulation

In this part of the report, we assess whether DJR can effectively recover its critical ICT systems and data if a disruption occurs.


DJR's disaster recovery processes are not robust enough to effectively and efficiently recover all critical systems after a disruption. DJR currently only has capability to recover selected critical systems. The department needs to do additional work to further develop its disaster recovery processes and capabilities to minimise any loss of critical services in the event of a disruption.

5.1 Business impact analysis

DJR's Crisis and Continuity Policy requires business units to review and update their business continuity plans annually, including BIAs.

Figure 5A summarises our assessment of DJR's BIA process and its components against COBIT 5 ISO/IEC 15504-based capability levels and a rating system based on the ISO/IEC 15504-2:2003 standard—see Appendix B for descriptions of the capability ratings.

Figure 5A
Assessment of DJR's BIA process and components

BIA process—overall capability 	
Component	Capability rating
List all of the critical business processes that underpin achievement of the agency's objectives	Largely achieved
Rank the processes in order of importance to the agency's objectives and exclude those processes not considered critical to achieving the objectives	Partially achieved
Consider process interdependencies that exist.	Partially achieved
Determine the minimum requirements necessary to perform each critical process	Largely achieved
Obtain executive endorsement of prioritised list of critical business processes	Largely achieved
Evaluate the impacts of a loss of each critical process according to the agency's objectives	Partially achieved
Identify interim processing procedures (alternative or manual processing) or techniques to be adopted during the recovery phase	Largely achieved
Determine the maximum allowable outage for each critical process	Largely achieved
Determine internal and external critical interdependencies	Partially achieved
Identify vital records	Partially achieved
Determine the recovery time objective for each critical business process and ICT system	Partially achieved
Determine the recovery point objective for data	Partially achieved
Obtain executive endorsement of the BIA	Largely achieved

Source: VAGO.

At DJR, 50 business units have a BIA, and five new business units are each developing one. DJR's BIA process does not:

- evaluate and rank the criticality of business processes relative to one another
- assess the impact of the loss of a critical business process
- identify and consider system dependency requirements when determining the maximum allowable outage time for business functions and recovery times for systems.

DJR needs to address these deficiencies in its BIA process to enable it to develop a more robust process.

When performing the annual BIA, business units do not always seek advice from DJR’s Knowledge, Information and Technology Services group about aligning the maximum allowable outage and recovery time objective with their systems and service delivery capabilities.

DJR has used its BIA process to identify critical system dependencies for all but one of its critical systems. It is currently working to address this gap—however, it does not have a criticality framework or guidance to support business units in performing these activities.

DJR is currently revising the BIA process to include an overarching BIA. This will help DJR to align its approaches to business continuity and disaster recovery, and create central oversight of business units’ assessments, enabling DJR to develop a department-wide approach.


5.2 Disaster recovery

DJR does not have a strategy, framework or policies for managing disaster recovery of its systems.

Within DJR, individual business units are responsible for ensuring appropriate disaster recovery arrangements for their systems. The Knowledge, Information and Technology Services group is responsible for disaster recovery arrangements for agency-wide systems. This group provides disaster recovery advice and support to business units if requested—although, to date, few business units have taken up this support. DJR has produced new guidance that recommends business units consult with the Knowledge, Information and Technology Services group.

Figure 5B summarises our assessment of DJR’s disaster recovery process and its components against COBIT 5 ISO/IEC 15504-based capability levels and ISO/IEC 15504–2:2003 respectively.

Figure 5B
Assessment of DJR’s disaster recovery process and components

Disaster recovery process—overall capability		
Component maturity	Capability rating	
Maintain an ICT disaster recovery continuity framework	Not achieved	
Review, maintain and improve the ICT disaster recovery plans	Partially achieved	
Conduct ICT disaster recovery plan testing	Partially achieved	
Conduct ICT disaster recovery training	Not achieved	

Source: VAGO.

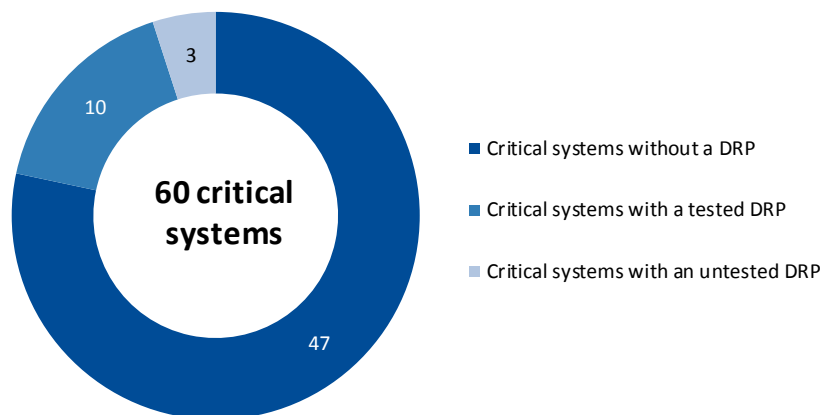
Disaster recovery plans and testing

DJR does not have full understanding of its systems' disaster recovery requirements. It conducted a review in July 2016 which found that, of its 60 critical systems, 13 have disaster recovery plans but 47 do not. The Knowledge, Information and Technology Services group is currently working with business units to validate existing disaster recovery requirements and develop new disaster recovery plans where needed.

Functional recovery tests performed by DJR verify whether it can recover the system, but not whether this can occur in line with business recovery requirements—because DJR has not determined them.

Figure 5C shows the number of systems supporting critical business functions at DJR that have a disaster recovery plan.

Figure 5C
DJR's critical systems and disaster recovery plans



Note: DRP = disaster recovery plan.

Source: VAGO, based on information from DJR.

Disaster recovery training

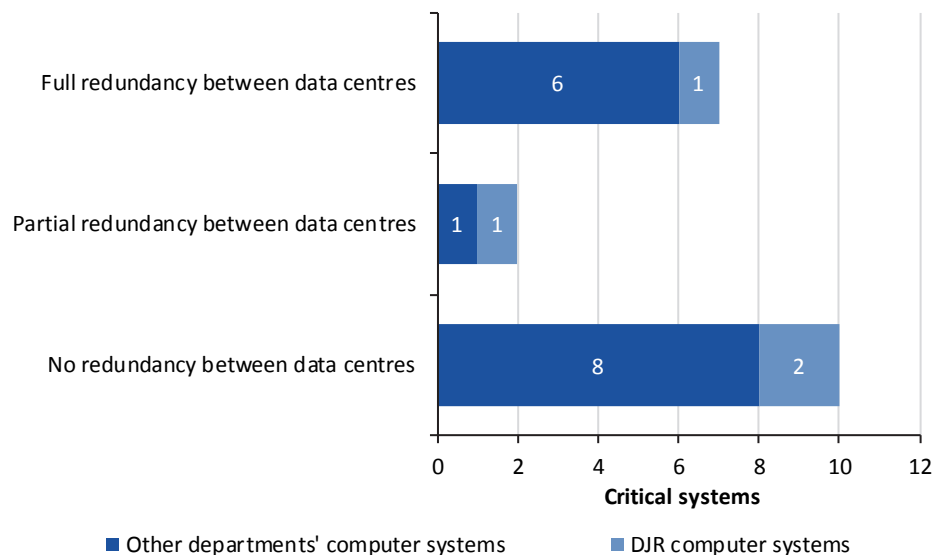
DJR performs functional disaster recovery tests on its critical systems but does not provide theoretical awareness training to staff with specific roles and responsibilities for disaster recovery.

Outsourced disaster recovery arrangement with CenITex

DJR engages CenITex for specific disaster recovery services, including annual disaster recovery testing and hosting disaster recovery capability of selected systems at the CenITex data centre. CenITex and DJR manage the terms and conditions of these specific disaster recovery services through statement-of-work documents.

Figure 5D shows the extent of redundancy capability in DJR's and the other audited agencies' critical systems hosted by CenITex.

Figure 5D
Redundancy capability in DJR's and other agencies' critical systems hosted by CenITex



Note: Nineteen of the 25 critical systems hosted by CenITex belong to the in-scope audited agencies.

Source: VAGO, based on data from CenITex.

Only one of DJR's four critical systems hosted by CenITex has redundancy capability. DJR does not have full visibility of the extent of its systems, and which ones have or need disaster recovery arrangements.

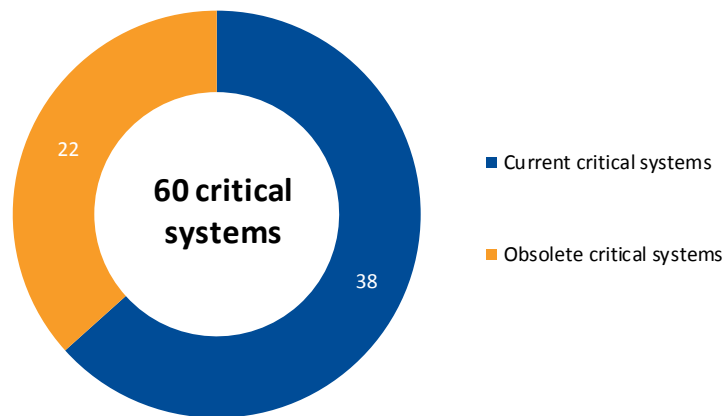
DJR is currently revising the BIA process to include an overarching BIA. This will help DJR align its approaches to business continuity and disaster recovery, and create central oversight of business unit assessments, enabling DJR to develop a department-wide approach. This will verify whether:

- the two systems hosted by CenITex that do not currently have redundancy capabilities need such capability
- the business requirements to have redundancy capabilities—partial or full—for the other two systems hosted at CenITex are still valid.

5.3 Obsolescence in systems

Figure 5E shows the number of obsolete systems supporting critical business functions as reported by DJR.

Figure 5E
Obsolete critical systems at DJR



Source: VAGO, based on information provided by DJR.

DJR's 2016 enterprise architecture review highlighted that, across all of the department's systems, only 55 were appropriate for future investment. The remaining 310 systems needed to be re-examined, upgraded, consolidated or decommissioned.

Due to DJR's model of individual business units being responsible for the life cycle management and asset register of their own systems, DJR does not have full visibility of the risks associated with the use of obsolete systems.

DJR's Knowledge, Information and Technology Services group is managing 22 specific projects and planning further projects to replace and upgrade selected systems and infrastructure, scheduled for completion by 2020. These projects are a reasonable way of reducing risk of obsolescence.

6

Victoria Police

In this part of the report, we assess whether Victoria Police can effectively recover its critical ICT systems and data if a disruption occurs.

Victoria Police's disaster recovery processes are not robust enough to effectively and efficiently recover all critical systems after a disruption. The agency currently only has capability to recover selected critical systems. Victoria Police needs to do additional work to further develop its disaster recovery processes and capabilities to minimise any loss of critical services in the event of a disruption.

6.1 Business impact analysis

In October 2016, an internal audit reported weaknesses in Victoria Police's ICT disaster recovery processes. The report found that Victoria Police:

- has not formally assessed critical business processes or functions to enable it to identify disaster recovery requirements to support business continuity
- does not have a disaster recovery framework, strategies, plans or processes
- does not have a defined and established test program and execution strategy.

Victoria Police has developed and started implementing a comprehensive plan to respond to the weaknesses identified in the audit, including:


- forming a governance committee and appropriate working groups
- performing a BIA to identify and review critical systems and ensure alignment between business requirements, recovery capabilities and disaster recovery strategy
- developing a disaster recovery framework, strategy and program.

It expects to complete this work by 31 December 2017.

Figure 6A summarises our assessment of Victoria Police's BIA process and its components against COBIT 5 ISO/IEC 15504-based capability levels and a rating system based on the ISO/IEC 15504-2:2003 standard—see Appendix B for descriptions of the capability ratings.

Figure 6A

Assessment of Victoria Police's BIA process and components

BIA process—overall capability 	
Component	Capability rating
List all critical business processes that underpin achievement of agency's objectives	Partially achieved
Rank the processes in order of importance to the agency's objectives and exclude those processes not considered critical to achieving the objectives	Partially achieved
Consider process interdependencies that exist	Partially achieved
Determine the minimum requirements necessary to perform each critical process	Partially achieved
Obtain executive endorsement of prioritised list of critical business processes	Partially achieved
Evaluate the impacts of a loss of each critical process according to the agency's objectives	Partially achieved
Identify interim processing procedures (alternative or manual processing) or techniques to be adopted during the recovery phase	Partially achieved
Determine the maximum allowable outage for each critical process	Partially achieved
Determine internal and external critical interdependencies	Partially achieved
Identify vital records	Partially achieved
Determine the recovery time objective for each critical business process and ICT system	Partially achieved
Determine the recovery point objective and data	Partially achieved
Obtain executive endorsement of the BIA	Not achieved

Source: VAGO.

Victoria Police is currently performing a BIA to:

- identify critical business functions, systems and resource dependencies
- determine maximum allowable outage for critical business functions
- determine recovery time and recovery point objectives for systems that support critical business functions
- analyse the operational and financial impacts of disruption to critical business functions
- assess risks and determine which critical systems need disaster recovery capabilities and, for systems that don't require disaster recovery capability, appropriate recovery strategies.

By August 2017, Victoria Police had performed a BIA for 30 of 78 business functions, with work continuing to address the remaining functions. The BIA will identify and gather key information that should help Victoria Police to:

- align system recoverability capabilities to business continuity requirements
- develop contingency plans to prepare for the loss of a business function
- identify opportunities for improvement and future technology upgrades, based on gap analysis of system and ICT service capabilities.

Victoria Police is taking appropriate steps to address its weaknesses. Completed BIAs have identified and gathered key information to help manage ICT disaster recovery planning.

System dependencies

Victoria Police, like many agencies, usually assesses a system's requirements in isolation and fails to consider each system's dependency on other systems when defining the recovery time objective and recovery point objective.

Figure 6B describes a case study about system dependencies for Victoria Police's custody management process.

Figure 6B

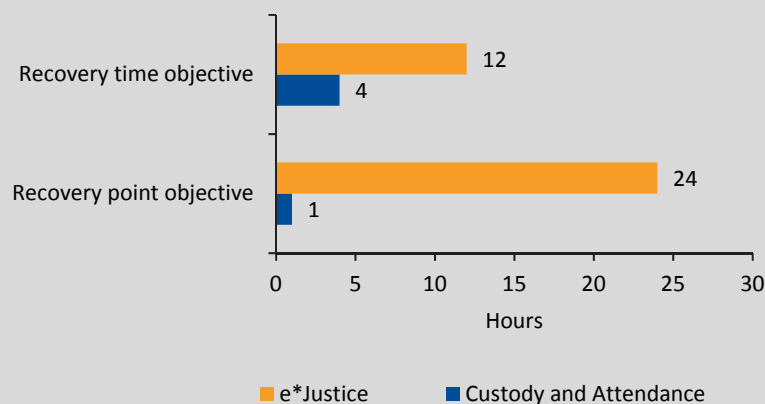
Case study: System dependencies for Victoria Police and DJR

Victoria Police uses the Attendance and Custody system for custody management, as part of operational policing. This system relies on information from DJR's e*Justice system, which DJR uses to manage evidence briefs and information about people accused of crimes.

The existing BIA processes of both agencies are inadequate for identifying dependent systems. The e*Justice system also has no disaster recovery capability. Both agencies have begun to address these weaknesses, including:

- establishing disaster recovery capability for the e*Justice system
- conducting a BIA to identify systems and their dependencies
- identifying recovery time and recovery point objectives for each system.

Currently, the recovery time and recovery point objectives of both systems do not align. This will increase the time required to recover the Attendance and Custody system if a disruption occurs, and will result in services being unavailable for longer than necessary.




Source: VAGO, based on information from Victoria Police and DJR.

6.2 Disaster recovery

Victoria Police has sought to address weaknesses in its disaster recovery processes by appointing an ICT Disaster Recovery Manager to help with internal initiatives and projects such as developing a disaster recovery framework and policies, and performing a gap analysis of disaster recovery requirements and the capabilities of resources and systems. Victoria Police has drafted a disaster recovery framework and policies, which are awaiting management endorsement.

Figure 6C summarises our assessment of Victoria Police's disaster recovery process and its components against COBIT 5 ISO/IEC 15504-based capability levels and ISO/IEC 15504–2:2003 respectively.

Figure 6C
Assessment of Victoria Police's disaster recovery process and components

Disaster recovery process—overall capability 	
Component	Capability rating
Maintain an ICT disaster recovery continuity framework, policy and strategy	Partially achieved
Review, maintain and improve the ICT disaster recovery plans	Partially achieved
Conduct ICT disaster recovery plan testing	Partially achieved
Conduct ICT disaster recovery training	Not achieved

Source: VAGO.

Victoria Police's disaster recovery processes require further improvement—they only support three key operational systems, and there is a lack of governance and strategic approach to disaster recovery across the agency.

Victoria Police recognises the need to further improve its management of disaster recovery as it upgrades existing systems to replace obsolete infrastructure.

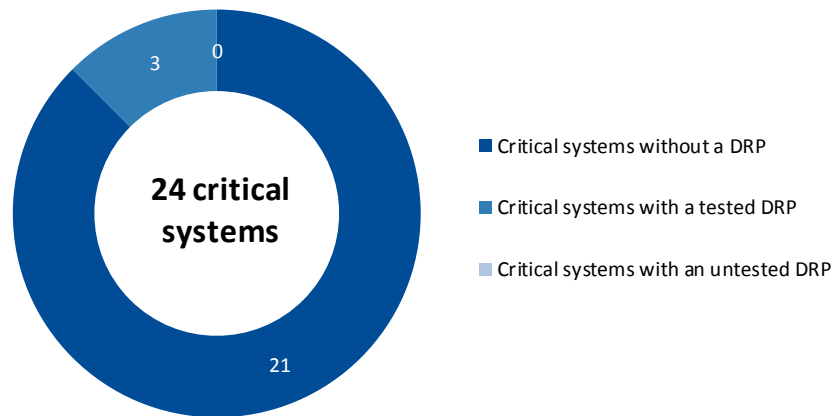
Victoria Police expects that its current work to address weaknesses will determine future disaster recovery investment and activities, and help to identify additional systems that need disaster recovery capability. Victoria Police intends to report and monitor progress of this work monthly in internal governance forums.

Disaster recovery plans and testing

Victoria Police has not yet identified all of its critical systems and determined whether they need disaster recovery capability.

Disaster recovery plans exist for only three of Victoria Police's 24 systems that support critical business functions. Victoria Police has tested all three of these plans, as shown in Figure 6D.

Figure 6D
Victoria Police's critical systems and disaster recovery plans



Note: DRP = disaster recovery plan.

Source: VAGO, based on information from Victoria Police.

Of the three Victoria Police systems that have disaster recovery plans:

- one system is supported by annual functional disaster recovery tests
- the other two systems are subject to discretionary functional disaster recovery tests, but these do not occur annually.

Victoria Police has formally set out disaster recovery arrangements in a contract with its main third-party ICT service provider to support and perform functional disaster recovery tests for these systems.

Functional recovery tests only verify that Victoria Police can recover a system, but they do not verify whether it can recover the system in line with business recovery requirements—because Victoria Police has not determined these requirements.

Victoria Police has not tested whether it can recover the remaining 21 critical systems, and no disaster recovery plans exist for these systems. Victoria Police advised that completion of the BIA review will identify whether any additional systems need disaster recovery capabilities and will inform decision-making on future disaster recovery investment and activities.

Disaster recovery training

Victoria Police does not provide theoretical disaster recovery awareness training for staff with specific roles and responsibilities for disaster recovery.

Data centre arrangement

Victoria Police hosts its systems at its operational site. It has other secondary data centre facilities, which can mitigate the risk and provide redundancy capabilities for these systems.

There is a risk that disruptions affecting the operational site—such as a fire—will also affect the systems hosted in the same building. Victoria Police is currently in the process of relocating its systems to a separate data centre facility, which it expects to complete by 2020.

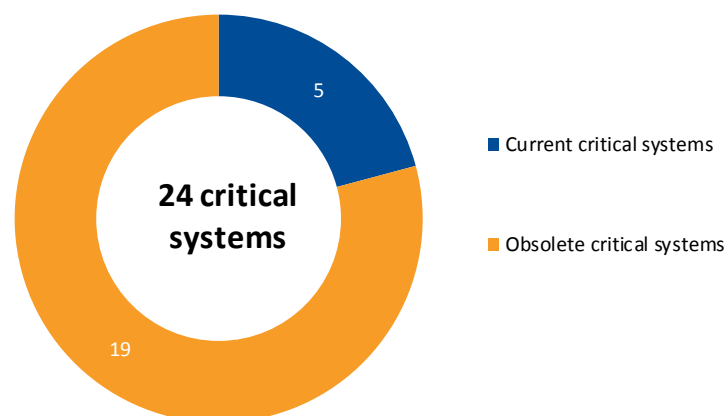
Victoria Police intends to enhance the disaster recovery capability of all critical systems by 31 December 2018 in preparation for the data centre relocation. However, the risk will remain until the move is finished.

6.3 Obsolescence in systems

One of the objectives in Victoria Police’s 2016–17 Business Technology Strategy is to review existing systems to verify their operational sustainability.

Figure 6E shows the number of systems supporting critical business functions in Victoria Police that it identifies as obsolete.

Figure 6E
Obsolete critical systems in Victoria Police



Source: VAGO, based on information from Victoria Police.

In 2016, Victoria Police upgraded the ICT infrastructure at its data centre to create a new technology platform for hosting and supporting future system upgrades and investment.

Victoria Police advised it will consider the investment priorities identified in its Business Technology Strategy review for replacing outdated and unsupported systems that are currently still in use.

Victoria Police is currently upgrading seven critical systems and one further system it classifies as vital, as part of its Infrastructure Lifecycle Program. It plans to replace these systems between 2020 and 2025, using its new technology platform.

Victoria Police has not effectively managed the risk of system obsolescence, as shown by the high percentage of its critical systems that are obsolete. Victoria Police needs to manage system obsolescence more effectively, using its Business Technology Strategy and Infrastructure Lifecycle Program to continuously improve its processes for identifying and managing obsolescence issues.

Appendix A

Audit Act 1994 section 16— submissions and comments

We have consulted with DEDJTR, DELWP, DHHS, DJR and Victoria Police, and we considered their views when reaching our audit conclusions. As required by section 16(3) of the *Audit Act 1994*, we gave a draft copy of this report, or relevant extracts, to those agencies and asked for their submissions and comments. We also provided a copy of the report to the Department of Premier and Cabinet.

Responsibility for the accuracy, fairness and balance of those comments rests solely with the agency head.

Responses were received as follows:

DEDJTR.....	66
DELWP	69
DHHS.....	70
DJR.....	75
Victoria Police	78

RESPONSE provided by the Secretary, DEDJTR



Department of Economic Development,
Jobs, Transport and Resources

GPO Box 4509
Melbourne Victoria 3001 Australia
Telephone: 03 9661 9999
www.economicdevelopment.vic.gov.au
DX 210074

Mr Andrew Greaves
Auditor-General of Victoria
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC. 3000

Dear Mr Greaves

VAGO's Proposed Performance Audit Report ICT Disaster Recovery Planning

Thank you for your letter on 3 November 2017, providing the Department with your proposed report on *ICT Disaster Recovery Planning*. We welcome the opportunity to provide comments.

The Department is committed to continuously improve the Department's disaster recovery planning. Whilst we have the capability to recover selected critical systems, additional work is required to further develop our disaster recovery processes and capabilities to minimise any loss to business services. Implementation of the Department's Business Continuity Framework and maturing the Department's IT disaster recovering planning is our priority. We accept VAGO's recommendations and the Department's response is enclosed.

Should you require any further information, please contact Alex Jones, Chief Information Officer on 03 8392 5936 or via email: alex.jones@ecodev.vic.gov.au.

Yours sincerely

Richard Bolt
Secretary

15 / 11 / 17



RESPONSE provided by the Secretary, DEDJTR—continued

Attachment C - DEDJTR's response to VAGO's recommendations – ICT Disaster Recovery Planning

No.	VAGO Recommendation	DEDJTR- Response
1	<p>Appoint a team of suitably qualified and experienced professionals to form a collaborative disaster recovery working group to:</p> <ul style="list-style-type: none"> - provide advice and technical support - share lessons learnt based on disaster recovery tests and exercises - coordinate disaster recovery requirements for resources shared between agencies - identify, develop, implement and manage initiatives that may impact multiple agencies - coordinate funding requests to ensure critical investments and requirements are prioritised. 	<p>Recommendation accepted in principle.</p> <p>The Department will participate and contribute in an appropriate state-wide working group for ICT disaster recovery.</p> <p>Action Date: Ongoing</p>
2	<p>DEDJTR to perform a gap analysis on their disaster recovery requirements and resource capabilities to determine the extent of the capability investment that will be required.</p>	<p>Recommendation accepted.</p> <p>The Department will review disaster recovery requirements following completion of its Business Continuity Framework.</p> <p>Action Date: 30 June 2018</p>
3	<p>DEDJTR to develop disaster recovery plans for the systems that support critical business functions and test these plans according to the disaster recovery test program.</p>	<p>Recommendation accepted.</p> <p>The Department will use the requirements identified in business continuity plans to develop and test disaster recovery plans of systems that support critical business functions.</p> <p>Action Date: 30 June 2018</p>
4	<p>DEDJTR to provide advice and training to staff on:</p> <ul style="list-style-type: none"> - newly developed frameworks, policies, standards and procedures to increase awareness and adoption as needed - specific disaster recovery systems. 	<p>Recommendation accepted.</p> <p>As noted above, the Department is developing an ICT Disaster Recovery Framework, in which training accountabilities and responsibilities will be documented and communicated to relevant parties.</p> <p>Action Date: 30 June 2018</p>

RESPONSE provided by the Secretary, DEDJTR—continued

5	<p>DEDJTR to establish system obsolescence management process:</p> <ul style="list-style-type: none"> - identify and manage systems at risk of becoming obsolete, those that will soon have insufficient support or those that will be difficult to manage when they become obsolete - enable strategic planning, life-cycle optimisation and the development of long-term business cases for system life-cycle support - provide executive with information to allow risk-based investment decisions to be made. 	<p>Recommendation accepted.</p> <p>The Department will establish a system obsolescence management process as part of the IT System Governance Framework to enable efficient management of ICT systems' life cycles across the Department.</p> <p>Action Date: 30 June 2018</p>
6	<p>DEDJTR to set up disaster recovery frameworks to provide guidelines and minimum standards for ICT disaster recovery planning, including:</p> <ul style="list-style-type: none"> - developing a strategy to establish the minimum levels of readiness and appropriate governance oversight - establishing the requirements, frequency and format of disaster recovery tests based on systems' criticality - establishing policies, standards and procedures for a consistent approach. 	<p>Recommendation accepted.</p> <p>Work to establish an ICT Disaster Recovery Framework and guidelines have commenced. These will enable a standardised approach for planning, implementing and managing disaster recovery requirements.</p> <p>Action Date: 31 January 2018</p>

RESPONSE provided by the Secretary, DELWP



Department of Environment,
Land, Water and Planning

PO Box 500, East Melbourne,
Victoria 8002 Australia
delwp.vic.gov.au

Mr Andrew Greaves
Auditor-General
Level 31 / 35 Collins Street
MELBOURNE VIC 3000

Ref: SEC013235



Dear Mr Greaves

PROPOSED PERFORMANCE AUDIT REPORT ICT DISASTER RECOVERY PLANNING

Thank you for your letter dated 3 November 2017 inviting the Department of Environment, Land, Water and Planning (DELWP) to provide a submission for inclusion in the report of the performance audit *ICT Disaster Recovery Planning*.

DELWP welcomes the report and agrees that effective disaster recovery capabilities are needed. It also supports the connection between effective disaster recovery planning and business continuity planning. The department notes that the lack of consistency in disaster recovery planning is largely a result of inadequate lifecycle management of information and communications technology (ICT), which we are now addressing by undertaking a criticality assessment of our ICT assets and developing a subsequent strategy.

I note that the report's conclusions with respect to DELWP are based on a figure of 80 critical systems, and that this has been determined by directly correlating the criticality of the system to the criticality of the business function the system supports. For DELWP, it is sometimes the case that a critical business function may be supported by a combination of critical and non-critical systems. Since the audit commenced, DELWP has begun an assessment of its ICT assets (including systems) under its ICT Criticality Framework. This framework measures the critical nature of its assets in relation to the risks of them not being available. We believe that this approach will clarify the extent of DELWP's critical ICT assets and how they are being managed. The initial results of the assessment points to approximately 60 critical assets. DELWP would welcome the opportunity to further respond to the audit's findings once we have concluded our own assessment.

DELWP accepts those recommendations that relate to it, and notes the issues identified in the report will be addressed by the criticality assessment of our ICT assets and the strategy that will be developed in response to its findings.

DELWP expects to complete the assessment and the evaluation of the results by the end of December 2017. Its ICT Committee will oversee the implementation of the resulting strategy during 2018.

DELWP also looks forward to continuing to work with the other audited departments to enhance our disaster recovery planning capabilities.

Please contact Claire Foo, the Chief Information Officer, DELWP, at Claire.Foo@delwp.vic.gov.au, if you wish to discuss our response further.

Yours sincerely

John Bradley
Secretary

201112017

Any personal information about you or a third party in your correspondence will be protected under the provisions of the *Privacy and Data Protection Act 2014*. It will only be used or disclosed to appropriate Ministerial, Statutory Authority, or departmental staff in regard to the purpose for which it was provided, unless required or authorized by law. Enquiries about access to information about you held by the Department should be directed to foi.unit@delwp.vic.gov.au or FOI Unit, Department of Environment, Land, Water and Planning, PO Box 500, East Melbourne, Victoria 8002.



RESPONSE provided by the Secretary, DHHS



Secretary

Department of Health and Human Services

50 Lonsdale Street
Melbourne Victoria 3000
Telephone: 1300 650 172
GPO Box 4057
Melbourne Victoria 3001
www.dhhs.vic.gov.au
DX 210081

e4679539

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3000


Dear Mr Greaves

Thank you for your letter of 3 November 2017 providing us with the proposed report for the *ICT Disaster Recovery Planning* audit.

I accept and welcome your recommendations to improve our disaster recovery capability. Please find enclosed the actions my department will take to address the report's recommendations.

In recognition that there is more work to be done on our disaster recovery capabilities, the department has made progress towards improving these capabilities by:

1. Establishing a Disaster Recovery and Business Continuity Planning Reference Group in July 2017 to ensure a well-managed and coordinated approach to disaster recovery investments and requirements;
2. Approving additional funding to develop and implement a disaster recovery strategy for the department; and
3. Performing a gap analysis of the 20 systems that support the department's business functions to identify and assess their disaster recovery capability and requirements.

I thank your staff for their work and the professional manner in which they engaged with my department on this audit.

I look forward to using your report to further improve our disaster recovery capability.

Yours sincerely


Kym Peake
Secretary

16 / 11 / 2017



ATTACHMENT

DHHS Action plan to the VAGO performance audit, ICT Disaster Recovery Planning Performance Audit

No	Recommendation	DHHS action	Proposed start date	Proposed end date
1	<p>Appoint a team of suitably qualified and experienced professionals to form a collaborative disaster recovery working group to:</p> <ul style="list-style-type: none"> provide advice and technical support share lessons learnt based on disaster recovery tests and exercises coordinate disaster recovery requirements for resources shared between agencies identify, develop, implement and manage initiatives that may impact multiple agencies coordinate funding requests to ensure critical investments and requirements are prioritised 	<p>Accept</p> <p>The department established a Disaster Recovery and Business Continuity Planning Reference Group in July 2017 to address the matters identified.</p> <p>The department will review the Terms of Reference, membership and performance of the Reference Group in December 2017 to ensure it is addressing the matters identified.</p>	July 2017	December 2017
2	<p>Perform a gap analysis on the disaster recovery requirements and resource capabilities to determine the extent of the capability investment that will be required</p>	<p>Accept</p> <p>The department will complete existing work to perform a gap analysis of the 20 key business systems' disaster recovery capability and requirements.</p>	September 2017	June 2018
3	<p>Develop disaster recovery plans for the systems that support critical business functions and test these plans according to the disaster recovery test program</p>	<p>Accept</p> <p>Disaster recovery plans currently exist for 11 systems managed by Business Technology and Information Management, and the branch performs annual functional disaster recovery tests on these systems.</p> <p>The gap analysis will assess the disaster recovery capabilities and requirements of each critical business function and</p>	September 2017	December 2018

ATTACHMENT

DHHS Action plan to the VAGO performance audit, *ICT Disaster Recovery Planning Performance Audit*

No	Recommendation	DHHS action	Proposed start date	Proposed end date
		determine which system/s require disaster recovery plans and associated testing. As a result, the Disaster Recovery and Business Continuity Planning Reference Group will oversee that the required disaster recovery systems and plans are developed and regular testing is performed.		
4	Provide advice and training to staff on: <ul style="list-style-type: none"> newly developed frameworks, policies, standards and procedures to increase awareness and adoption as needed on specific disaster recovery systems 	Accept Training and guidance will be provided to specific business units within the branch and system business owners, once the deliverables from the gap analysis have been implemented.	June 2018	December 2018
5	Establish system obsolescence management processes to: <ul style="list-style-type: none"> identify and manage systems at risk of becoming obsolete, those that will soon have insufficient support or those that will be difficult to manage when they become obsolete enable strategic planning, life-cycle optimisation and the development of long-term business cases for system life-cycle support provide executive with information to allow risk-based investment decisions to be made. 	Accept The department will continue to implement proactive and strategic management processes to identify and plan for the management of obsolete systems, through the department's Enterprise Architecture. The department's Enterprise Architecture identifies which systems are obsolete or approaching their end of life and informs the risk-based prioritisation approach for system upgrade or replacement. This is incorporated in the department's ICT investment program as part of the annual ICT planning process. Each investment is assessed and	November 2017	June 2018

ATTACHMENT

DHHS Action plan to the VAGO performance audit, *ICT Disaster Recovery Planning Performance Audit*

No	Recommendation	DHHS action	Proposed start date	Proposed end date
6	<p>Set up disaster recovery frameworks to provide guidelines and minimum standards for ICT disaster recovery planning, including:</p> <ul style="list-style-type: none"> developing a strategy to establish the minimum levels of readiness and appropriate governance oversight establishing the requirements, frequency and format of disaster recovery tests based on systems' criticality establishing policies, standards and procedures for a consistent approach 	<p>prioritised against competing ICT investment needs. The risk-based view of the department's Enterprise Architecture will inform the prioritisation for the annual ICT investment planning for the 2018-19 financial year.</p> <p>Accept</p> <p>The Disaster Recovery and Business Continuity Planning Reference Group has been established to develop a disaster recovery framework and strategy, to ensure a well-managed and coordinated approach to disaster recovery requirements.</p> <p>As a result, the department will:</p> <ul style="list-style-type: none"> complete existing work to perform a gap analysis to determine the minimum standards for ICT disaster recovery, develop and implement frameworks, policies and standards to support the department's recovery objectives and ensure compliance. 	September 2017	December 2018
9	Update its Business Continuity Policy to require business units to consult with system owners and the Business Technology and Information Management group as part of the business impact analysis process, to validate the maximum allowable outage and recovery time objectives	<p>Accept</p> <p>The Disaster Recovery and Business Continuity Planning Reference Group will oversee that the Business Continuity Policy will be updated, as a result of the outcome of the gap analysis.</p> <p>The Emergency Management branch and Business Technology and Information Management branch will work closely with system business owners to determine their</p>	June 2018	December 2018

ATTACHMENT

DHHS Action plan to the VAGO performance audit, ICT Disaster Recovery Planning Performance Audit

No	Recommendation	DHHS action	Proposed start date	Proposed end date
10	Update the business impact analysis process to identify system dependencies for critical business functions	Accept The department's business impact analysis processes will be updated as a result of the outcome of the gap analysis, which will identify the system dependencies for each critical business function. The Disaster Recovery and Business Continuity Planning Reference Group will manage the implementation of this activity.	June 2018	December 2018
11	Determine a recovery strategy of systems that support critical business functions.	Accept The outcome of the gap analysis will determine what is the appropriate recovery strategy of each system that supports critical business functions. The Disaster Recovery and Business Continuity Planning Reference Group will ensure each system has an acceptable recovery strategy developed and implemented.	June 2018	December 2018

RESPONSE provided by the Secretary, DJR



Department of Justice and Regulation

Secretary

121 Exhibition Street
Melbourne Victoria 3000
GPO Box 4356
Melbourne Victoria 3001
Facsimile: (03) 8684 0525
justice.vic.gov.au
DX: 210220

17 NOV 2017

Our ref: CD/17/648766

Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE, VIC, 3000

Dear Mr Greaves

Proposed Audit Report: ICT Disaster Recovery Planning

Thank you for your letter dated 3 November 2017 enclosing the proposed audit report *ICT Disaster Recovery Planning*, and the invitation to provide a formal response.

The Department of Justice and Regulation (the department) recognises that ICT systems are critical for the operations of government agencies and is committed to making sure that its systems remain available and continue to operate reliably.

The department notes the report's findings that it needs to strengthen its ICT disaster recovery activities and accepts all of the recommendations directed to it. An action plan to implement the recommendations is provided at Attachment A.

Thank you again for the opportunity to provide comment.

Yours sincerely

Greg Wilson
Secretary

Encl. Proposed Action Plan – ICT Disaster Recovery Planning

cc: Ms Annabel Brebner, Director, Performance Audit



RESPONSE provided by the Secretary, DJR—continued

ICT Disaster Recovery Planning

Department of Justice and Regulation response to VAGO recommendations

Recommendation	Proposed Action	Completion Date
<u>Recommendation 1</u> Appoint a team of suitably qualified and experienced professionals to form a collaborative disaster recovery working group to: <ul style="list-style-type: none"> • provide advice and technical support • share lessons learnt based on disaster recovery tests and exercises • coordinate disaster recovery requirements for resources shared between agencies • identify, develop, implement and manage initiatives that may impact multiple agencies • coordinate funding requests to ensure critical investments and requirements are prioritised 	Accept Subject to the establishment of a whole-of-Victorian-government disaster recovery working group, the department will commit suitably qualified and experienced professionals to participate in it.	December 2018
<u>Recommendation 2</u> Perform a gap analysis on their disaster recovery requirements and resource capabilities to determine the extent of the capability investment that will be required	Accept A current state assessment, including gap analysis on the disaster recovery requirements and resource capabilities, will be undertaken to support the Disaster Recovery Strategy (see Recommendation 6).	December 2018
<u>Recommendation 3</u> Develop disaster recovery plans for the systems that support critical business functions and test these plans according to the disaster recovery test program	Accept The department will implement: <ul style="list-style-type: none"> • a central register to maintain DR plans for critical systems • a twice-yearly process to monitor the completion and testing of DR plans 	December 2018
<u>Recommendation 4</u> Provide advice and training to staff on: <ul style="list-style-type: none"> • newly developed frameworks, policies, standards and procedures to increase awareness and adoption as needed • specific disaster recovery systems 	Accept A communications plan will be developed to ensure that all business areas and key stakeholders are informed of the strategy, policies, standards, procedures and systems.	December 2018
<u>Recommendation 5</u> Establish system obsolescence management processes to: <ul style="list-style-type: none"> • identify and manage systems at risk of becoming obsolete, those that will soon have insufficient support or those that will be difficult to manage when they become obsolete • enable strategic planning, life-cycle optimisation and the development of long-term business cases for system life-cycle support • provide executive with information to allow risk-based investment decisions to be made 	Accept The department will develop a regular report of systems which are obsolete or at risk of becoming obsolete. This information will be provided to system owners and business unit directors to use as part of existing strategic and investment planning processes. The department will also develop guidance, communications and processes to ensure: <ul style="list-style-type: none"> • obsolescence is managed effectively • business cases for new technology includes lifecycle consideration and risk management to inform investment decisions 	December 2018

RESPONSE provided by the Secretary, DJR—continued

Recommendation	Proposed Action	Completion Date
Recommendation 6 Set up disaster recovery frameworks to provide guidelines and minimum standards for ICT disaster recovery planning, including: <ul style="list-style-type: none"> developing a strategy to establish the minimum levels of readiness and appropriate governance oversight establishing the requirements, frequency and format of disaster recovery tests based on systems' criticality establishing policies, standards and procedures for a consistent approach 	Accept The department will develop a Disaster Recovery Strategy which will establish the requirements for disaster recovery planning and recovery testing for critical business systems. This strategy will be supported by standards, guidelines and tools as required.	December 2018
Recommendation 12 Update its Crisis and Continuity Policy to require business units to consult with system owners and the Knowledge, Information and Technology Services group as part of the business impact analysis process, to validate the maximum allowable outage and recovery time objectives	Accept The department will update the Crisis and Continuity Policy to include a consultation process to ensure alignment between recovery time objectives and maximum allowable outages for critical services.	June 2018
Recommendation 13 Develop a framework to assist business units to determine the criticality of business functions and identify disaster recovery requirements	Accept The department will develop assessment criteria to determine criticality of key services as part of its business impact analysis process. The Disaster Recovery Strategy (as per Recommendation 6) will identify disaster recovery requirements aligned to service criticality.	June 2018
Recommendation 14 Determine a recovery strategy for systems that support critical business functions	Accept As per Recommendations 3 and 6, the department will develop: <ol style="list-style-type: none"> a Disaster Recovery Strategy Disaster Recovery Plans for critical systems 	June 2018 Nov 2018
Recommendation 15 Update the business impact analysis process to include components that: <ul style="list-style-type: none"> evaluate and rank the criticality of business functions analyse impacts caused by disruption to critical business functions 	Accept As per Recommendation 12, the department will update its BIA process to include analysis of disruption impacts.	June 2018

CD/17/629467

RESPONSE provided by the Acting Chief Commissioner, Victoria Police



VICTORIA POLICE

Chief Commissioner's Office

Victoria Police Centre
637 Flinders Street
Docklands 3008
Victoria Australia
Telephone (61 3) 9247 6890
Facsimile (61 3) 9247 6869

PO Box 913
Melbourne 3001
Victoria Australia

Our Ref: FF-109951
Your Ref: 32655

Mr Andrew Greaves
Victorian Auditor General
GPO Box 24234
Melbourne Vic 3001

Dear Mr Greaves

Performance Audit Report ICT Disaster Recovery Planning

Thank you for your letter dated 3 November 2017 and the Draft Report for the performance audit on ICT Disaster Recovery Planning.

While Victoria Police accepts the findings, it is important to note we have already commenced a significant program of work to enhance our disaster recovery capability.

Please find attached a summary of proposed Victoria Police actions and anticipated completion dates (Attachment A).

Yours sincerely

A handwritten signature in black ink, appearing to be 'Andrew Crisp', written over a horizontal line.

Andrew Crisp APM
Acting Chief Commissioner

16 / 11 / 2017

**RESPONSE provided by the Acting Chief Commissioner, Victoria Police—
continued**

For Official Use Only

ATTACHMENT A

**Proposed Victoria Police actions in response to Recommendations from the
Performance Audit Report on ICT Disaster Recovery Planning**

Rec No.	Recommendation	Proposed Victoria Police Action	Anticipated Completions Dates
1	Appoint suitably qualified & experienced professionals	IT Service Provider is appointing a suitably qualified Disaster Recovery manager.	December 2017
2	Perform gap analysis	A Business Impact Assessment (BIA) of enterprise capabilities is 90% complete. Upon completion, the BIA findings will be fully embedded within Victoria Police's Enterprise Risk Framework and Business Continuity Reform Program.	December 2017
3	Develop DR plans and test	<p>A DR plan and test program to enhance capability of all critical systems will be completed by the end of 2018 in preparation for VPC Data Centre site relocation.</p> <p>A full site failover for the LEAP mainframe and application has been successfully conducted. This result proves that VP can recover its most critical application from an event in less than 2 hours (within business expectations). <i>(Completed after audit closure)</i></p>	December 2020
4	Provide advice and training	Ongoing advice and training will be conducted during the development of the Disaster Recovery capability, the writing of the DR plans and subsequent DR testing program.	Commenced/Ongoing Program
5	Establish program to manage system obsolescence	Victoria Police continue to implement a lifecycle program to mitigate obsolescence of all critical IT systems, including DR technical deficit.	Critical systems complete December 2020
6	Set up DR frameworks	<p>A DR policy/framework and test strategy has been completed and is pending endorsement.</p> <p>Technical design patterns have been drafted to provide consistent repeatable and robust solutions to achieve Disaster Recovery requirements and will be finalised by Dec 2017.</p>	December 2017







Page 2 of 2

For Official Use Only

Appendix B

Capability levels and descriptions

Figure B1
Capability levels and descriptions based on COBIT 5 ISO/IEC 15504 capability levels

Capability level	Description
 Incomplete	Process not in place or it cannot achieve its objective
 Performed	Process in place and achieves its purpose
 Managed	Process implemented in a managed way and appropriately controlled and maintained
 Established	Process implemented using a defined process that is capable of achieving its outcomes
 Predictable	Process operates within defined limits to achieve its outcomes
 Optimised	Process continuously improved to meet relevant current and projected enterprise goals

Source: VAGO, based on COBIT 5 ISO/IEC 15504 capability levels.

Figure B2
Process components based on the ISO/IEC 15504-2:2003 standard

Rating	Description	Achievement (percentage)
Not achieved	Little or no evidence of achievement of the defined component of the process	0–15% achievement
Partially achieved	Some evidence of an approach to and achievement of the defined component of the assessed process	>15–50% achievement
Largely achieved	Evidence of a systematic approach and significant achievement of the process, with some opportunities for improvement remaining	>50–85% achievement
Fully achieved	Evidence of a complete and systematic approach and full achievement of the component of the assessed process, with no significant remaining weaknesses	>85% achievement

Source: VAGO, based on ISO/IEC 15504-2:2003 standard.

Auditor-General's reports tabled during 2017–18

Report title	Date tabled
V/Line Passenger Services (2017–18:1)	August 2017
Internal Audit Performance (2017–18:2)	August 2017
Effectively Planning for Population Growth (2017–18:3)	August 2017
Victorian Public Hospital Operating Theatre Efficiency (2017–18:4)	October 2017
Auditor-General's Report on the Annual Financial Report of the State of Victoria, 2016–17 (2017–18:5)	November 2017
Results of 2016–17 Audits: Water Entities (2017–18:6)	November 2017
Results of 2016–17 Audits: Public Hospitals (2017–18:7)	November 2017
Results of 2016–17 Audits: Local Government (2017–18:8)	November 2017

All reports are available for download in PDF and HTML format on our website www.audit.vic.gov.au

Victorian Auditor-General's Office
Level 31, 35 Collins Street
Melbourne Vic 3000
AUSTRALIA

Phone +61 3 8601 7000
Email enquiries@audit.vic.gov.au